

Zusammenstellung sicherheitstechnischer Anforderungen an Interfaces der Mess- und Stelltechnik in software-basierten Leitechniksystemen mit sicherheitstechnischer Bedeutung in Kernkraftwerken

**Abschlussbericht
zu dem Vorhaben SR 2499**

erstellt von

**TÜV Industrie Service GmbH TÜV SÜD Gruppe
Energie und Technologie**

**Christian Michas
Cornelia Bühler**

November 2005

**Erstellt im Auftrag des Bundesministeriums für Umwelt, Naturschutz und
Reaktorsicherheit im Rahmen des Vorhabens SR 2499**

Der Auftraggeber behält sich alle Rechte vor. Insbesondere darf dieser Bericht nur mit seiner Zustimmung zitiert, ganz oder teilweise vervielfältigt bzw. Dritten zugänglich gemacht werden. Der Bericht gibt die Auffassung und Meinung des Auftragnehmers wieder und muss nicht mit der Meinung des Auftraggebers übereinstimmen.

Kurzfassung

Moderne Automatisierungssysteme bauen auf Bussystemen mit serieller Datenübertragung für den Austausch von Informationen auf. In diesem Forschungsvorhaben wird der Einsatz von digitaler Signalübertragung in der Leittechnik mit sicherheitstechnischer Bedeutung für die Kategorien A und B von Kernkraftwerken untersucht.

Es werden zunächst der derzeitige Stand der Sicherheitsbustechnik vorgestellt und die sich damit neu ergebenden Automatisierungsstrukturen speziell für den Sicherheitseinsatz aufgezeigt. Weiterhin werden wesentliche Aspekte für den Einsatz sicherheitsgerichteter Bussysteme in der Sicherheitsleittechnik von Kernkraftwerken analysiert und relevante Anforderungen zusammengestellt. Zur Berücksichtigung der speziellen Gegebenheiten und Anforderungen an Bus-Interfaces wurde der im Rahmen des Forschungsvorhabens SR 2422 „Anforderungen an rechnergestützte periphere Komponenten des Sicherheitssystems in Kernkraftwerken“ erstellte Fragenkatalog erweitert.

Zur näheren Betrachtung wurden zwei Typvertreter für Bus-Interface-Baugruppen ausgewählt und beschrieben. Für diese Typvertreter wurde der angepasste Fragenkatalog beantwortet und ausgewertet.

Mit den Ergebnissen werden grundlegende Informationen zum Einsatz von Sicherheitsbussen in sicherheitstechnisch relevanter Leittechnik zu Verfügung gestellt, die als Basis für die Begutachtung von Bussystemen z. B. im Rahmen von Modernisierungen in Kernkraftwerken dienen können.

Abstract

Modern I&C systems build on bus systems for data communication. In this research project the application of data communication in I&C systems important for safety performing category A and B functions of nuclear power plants is examined.

First the status of the safety bus technology and the resulting automation structures especially for the safety application are presented. Further substantial aspects for the application of safety bus systems in I&C systems important for safety of nuclear power plants are analyzed and relevant requirements are listed. For the consideration of the special conditions and requirements for bus interfaces the set of questions of the research project SR 2422 "Requirements for computer-based peripheral devices of the safety system in nuclear power plants" was extended.

For closer view two representatives for bus interface components were selected and described. For these representatives the adapted set of questions was answered and evaluated.

With these results basic aspects for the application of safety buses in I&C systems important for safety are provided for the evaluation of the use of buses in nuclear power plants.

Inhaltsverzeichnis

1	Einleitung	6
2	Auswirkungen auf die Automatisierungsstruktur	8
2.1	Bisherige Sensor-Aktor-Anbindung	8
2.2	Zukünftige Sensor-Aktor-Anbindung	9
3	Anforderungen an Interfaces	11
3.1	Ergebnis der Normenanalyse	11
3.2	Anpassung des Fragenkatalogs aus dem Vorhaben SR 2422	15
4	Einführung in die Sicherheitsbustechnologie	18
4.1	Neue Fehlertypen im Zusammenhang mit Buskommunikation	19
4.2	Konzept und Auslegung von Sicherheitsbussen	20
4.2.1	Grey-Channel.....	20
4.2.2	Ausbau bestehender Sicherheitsmechanismen (White Channel)	21
4.3	Darstellung der unterschiedlichen Buszugriffsverfahren	22
5	Beschreibung der Typvertreter	26
5.1	Marktrecherche und Auswahlkriterien	26
5.2	Typvertreter I: PROFIsafe Profil	31
5.2.1	Beschreibung	31
5.2.2	Umfang und Ergebnis der Typprüfung	34
5.2.3	Auswertung des Fragenkataloges.....	34
5.3	Typvertreter II: CANopen Safety Chip	36
5.3.1	Beschreibung	36
5.3.2	Umfang und Ergebnis der Typprüfung	39
5.3.3	Auswertung des Fragenkataloges.....	40
6	Zusammenfassung und Ausblick	42
7	Abkürzungsverzeichnis	44



8	Normenverzeichnis	46
9	Literaturverzeichnis.....	50

Anhang I: Ausgefüllter Fragenkatalog Typvertreter I

Anhang II: Ausgefüllter Fragenkatalog Typvertreter II

Anhang III: Anforderungen an Interfaces

III.1 Aufrechterhaltung des Defence-in-Deth-Konzeptes

III.2 Aufrechterhaltung der verfahrenstechnischen Redundanz der Anlage

III.3 Systemarchitektur

III.4 Gewährleistung der Unabhängigkeit der kommunizierenden Teilsysteme

III.5 Realisierung / Performance

III.6 Fehlererkennung und -beherrschung

III.7 Security

III.8 Kabel / Kabelverlegung

1 Einleitung

Rechnerbasierte Systeme prägen die Leittechnik im industriellen Umfeld bereits in hohem Maße. Auch im kerntechnischen Bereich gewinnen derartige Systeme immer mehr an Bedeutung. Die damit in Zusammenhang stehenden, verteilten und komplexeren industriellen Steuerungen erfordern einen höheren Umfang an auszutauschenden Daten zwischen den verschiedenen Geräten und Systemen. Die heute im kerntechnischen Bereich größtenteils eingesetzten elektrischen Einzelsignalleitungen zwischen den Komponenten werden aus technischen und wirtschaftlichen Gründen sowie aus Gründen der Beschaffung zunehmend durch Bussysteme abgelöst werden.

Um den Verdrahtungsaufwand moderner Automatisierungssysteme zu reduzieren, kommen im industriellen Umfeld verstärkt Interfaces auf Basis serieller Datenübertragung (Bussysteme) zum Einsatz. Für den Austausch von Daten zwischen verschiedenen Geräten bieten diese Datenverbindungen Vorteile gegenüber Systemen mit elektrischen Einzelleitungen. Neben dem geringeren Verdrahtungsaufwand zählen dazu die Möglichkeit für Parametrierung und Diagnose von Sensoren und Aktoren über das Bussystem sowie die flexiblere Gestaltung von Automatisierungsstrukturen durch unterschiedliche Netztopologien. Des Weiteren bieten diese Bussysteme einfache Erweiterungsmöglichkeiten. Dadurch bedingt entstehen grundlegend neue Konzepte bei der Auslegung von Automatisierungsstrukturen. Auf der anderen Seite werden durch die Verwendung von Bussystemen neuartige Fehlertypen verursacht, die beherrscht werden müssen.

Aufgrund des mittlerweile hohen Verbreitungsgrades von Bussystemen im industriellen Bereich und den gegebenen Vorteilen dieser Technik gegenüber konventioneller Verdrahtung stellt sich die Frage, unter welchen Bedingungen derartige Systeme im kerntechnischen Bereich Anwendung finden können. Im Rahmen dieses Forschungsvorhabens werden der derzeitige Stand der Sicherheitsbustechnik vorgestellt und neue Automatisierungsstrukturen speziell für den Sicherheitseinsatz gezeigt sowie die relevanten Anforderungen aus dem kerntechnischen Regelwerk zusammengestellt. Hierbei wird ins-



besondere der Einsatz in sicherheitstechnischer Leittechnik der Kategorien A und B gemäß IEC 61226 /N10/ betrachtet. Zur näheren Betrachtung werden zwei Typvertreter ausgewählt und detaillierter betrachtet. Für diese Typvertreter wird weiterhin der generische Fragenkatalog des Forschungsvorhabens SR 2422, der bezüglich der Thematik „Interfaces“ erweitert wurde, beantwortet.

2 Auswirkungen auf die Automatisierungsstruktur

Mit dem Einzug der digitalen Leittechnik in die Automatisierungstechnik im industriellen Bereich werden verstärkt Bussysteme für den Informationsaustausch zwischen den einzelnen Teilsystemen eingesetzt. Ein rechnerbasiertes Automatisierungssystem ist hierbei üblicherweise in drei Hierarchieebenen unterteilt. In der mittleren Hierarchieebene, der sog. Logikebene, sind die speicherprogrammierbaren Steuerungen (SPS) angeordnet, die die zentrale Bearbeitung der leittechnischen Funktionen übernehmen. In der oberen Hierarchieebene, der sog. Leitebene, kommunizieren Bedien- und Beobachtungsstationen, Engineering-Stationen und weitere Mensch-Maschine-Schnittstellen miteinander und mit der Logikebene. In der unteren Hierarchieebene, dem Feldbereich, befinden sich die an den Prozess angebundenen Sensoren und Aktoren, die mit der Logikebene und teilweise auch untereinander kommunizieren.

2.1 Bisherige Sensor-Aktor-Anbindung

Traditionelle, fest verdrahtete Automatisierungssysteme stellen die Kommunikation der räumlich getrennten Logikebene mit dem Feldbereich über elektrische Einzelverbindungen her (siehe Abbildung 1). Die Automatisierungsstruktur ist gekennzeichnet durch ei-

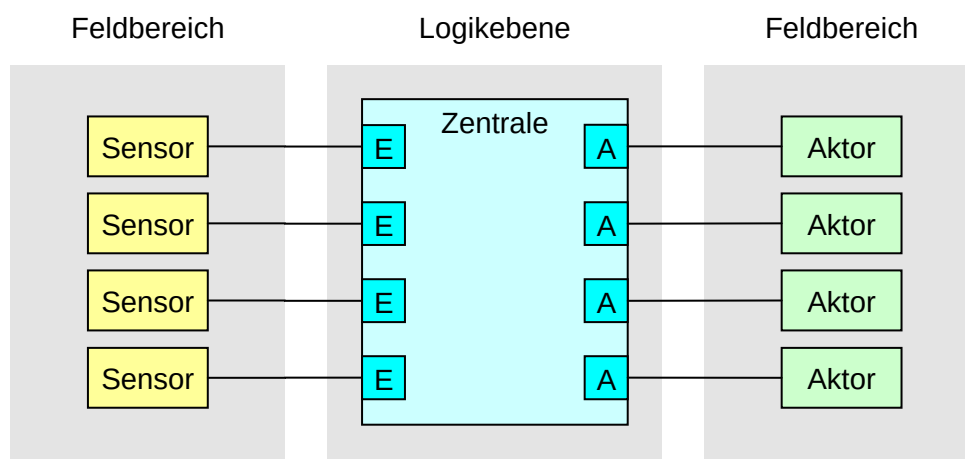


Abbildung 1: Bisherige Sensor-Aktor-Anbindung

nen zentralisierten Aufbau. Bei der Auslegung der Kommunikationsverbindung werden Sensoren und Aktoren über getrennte Ein- bzw. Ausgabemodule an die Logikebene angeschlossen.

2.2 Zukünftige Sensor-Aktor-Anbindung

Moderne industrielle Automatisierungsstrukturen verfolgen den Trend zur Dezentralisierung. Über Bussysteme werden die Ein-/Ausgabebaugruppen quasi in den Feldbereich, in die sog. dezentrale Peripherie verlagert (siehe Abbildung 2). Bei der Modernisierung von bestehenden Leittechniksystemen ist auch ein Mischbetrieb fest verdrahteter Ein-/Ausgabebaugruppen in der Zentrale und einer über Bussysteme angeschlossenen dezentralen Peripherie möglich. Die Anbindung der Peripherie an die Zentrale über Bussysteme erfolgt vornehmlich über sog. Busklemmen. Diese sind individuell konfigurierbar und können sowohl Ein- als auch Ausgangsbaugruppen aufnehmen. Die Aufteilung der Sensoren und Aktoren auf unterschiedliche periphere Busklemmen ist aufgabenangepasst möglich. Eine Strukturierung gemäß den Redundanzen ist für den kerntechnischen Einsatz hierbei erforderlich. Neben dieser Variante der dezentralen Peripherie als eine Art von Unterzentrale im Feld existieren bereits einige wenige Geräte mit direktem Busan-

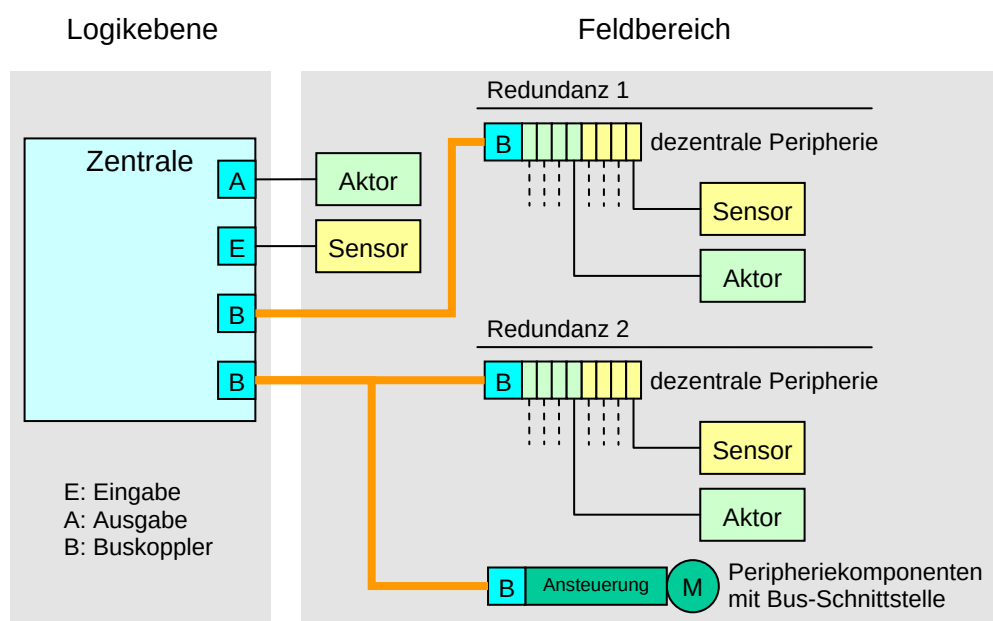


Abbildung 2: Zukünftige Sensor-Aktor-Anbindung

schluss (z. B. Motoransteuerungen).

Eine weitergehende Ausführungsform, die bereits in der Industrie eingesetzt wird, ist eine Systemarchitektur, die keine Zentrale mehr aufweist. Die Intelligenz ist dezentral im Feld verteilt und die Sensoren und Aktoren kommunizieren direkt untereinander über einen gemeinsamen Bus (siehe Abbildung 3). Diese Technik ist besonders sinnvoll in Bereichen, die geringe Logikkomplexität aufweisen. Die Reaktionszeiten können durch einen dezentralen Aufbau stark reduziert werden. Für den Einsatz in sicherheitskritischen Aufgaben kann ein sog. Sicherheitsmonitor als zentrale Überwachungsinstanz dem Netz hinzugefügt werden. Sobald er einen Komponentenausfall oder einen Kommunikationsfehler auf dem Bus erkennt, initiiert er definierte Fehlerreaktionen über fest verdrahtete Ausgänge.

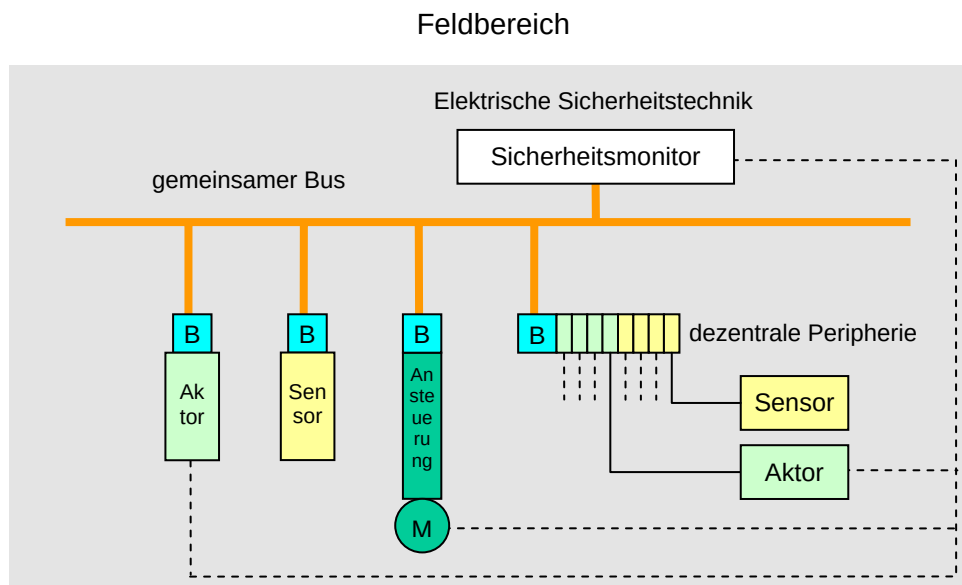


Abbildung 3: Logikebene dezentral im Feldbereich verteilt

3 Anforderungen an Interfaces

3.1 Ergebnis der Normenanalyse

Für die Zusammenstellung der für die Kerntechnik bestehenden Anforderungen an Interfaces wurden die normativen Dokumente des kerntechnischen Regelwerks analysiert und die relevanten Anforderungen extrahiert. Hierbei wurden in folgenden normativen Dokumenten relevante Anforderungen identifiziert:

- BMU/BMI-Sicherheitskriterien für Kernkraftwerke /N1/
- RSK-Leitlinien für Druckwasserreaktoren /N2/
- KTA 3501 Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems /N3/
- KTA 3904 Warte, Notsteuerstelle und örtliche Leitstände in Kernkraftwerken /N4/
- IAEA NS-R-1 Safety Requirements: Safety of Nuclear Power Plants: Design /N5/
- IAEA NS-G-1.1 Safety Guide: Software for Computer Based Systems Important to Safety in Nuclear Power Plants /N6/
- IAEA NS-G-1.3 Safety Guide: Instrumentation and Control Systems Important to Safety in Nuclear Power Plants /N7/
- IEC 60709 Kerntechnik – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Räumliche und elektrische Trennung /N8/
- IEC 60987 Digitalrechner für sicherheitstechnisch wichtige Systeme in Kernkraftwerken /N9/
- IEC 61226 Kernkraftwerke – Sicherheitsleittechnik – Kategorisierung /N10/
- IEC 61513 Kerntechnik – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen /N12/

- VDI/VDE 3527 Kriterien zur Gewährleistung der Unabhängigkeit von Sicherheitsfunktionen bei der Leittechnik-Auslegung /N13/
- DIN V VDE 0801 Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben /N14/

Die einzelnen Anforderungen sind im Anhang III aufgelistet. Für die Nachvollziehbarkeit wurden zu den Anforderungen die Angabe des zugrunde liegenden Dokuments und ein Stellenverweis angegeben. Bei Dokumenten, die nur in englischer Sprache verfügbar waren, wurden die Anforderungen übersetzt, um den Vergleich zwischen den Anforderungen aus den verschiedenen Dokumenten zu erleichtern¹. Zur näheren Einordnung wurden für die Anforderungen noch Zuordnungen zu den Kategorien A und B gemäß IEC 61226 vorgenommen.

Die Analyse der identifizierten Anforderungen ergab, dass folgende Themengebiete angesprochen werden:

- **Aufrechterhaltung des Defence-in-Depth-Konzeptes der Anlage**

Das Regelwerk fordert hierzu die Vermeidung von Verbindungen zwischen der Sicherheitsleittechnik unterschiedlicher Kategorien sowie zur Betriebsleittechnik. Für notwendige Verbindungen ist die Rückwirkungsfreiheit in Richtung des Systems der höherwertigen Kategorie sicherzustellen. Hierbei sind neben dem bestimmungsgemäßen Betrieb auch versagensauslösende Ereignisse zu berücksichtigen. Eine geforderte Maßnahme zur Umsetzung dieser Anforderung ist hierbei, dass der Datenfluss von den Systemen der höheren zu der niedrigeren Kategorie verlaufen soll. Weiterhin werden Vorkehrungen gegen Ausfallfortpflanzung über die Verbindungen, wie z. B. durch elektrische Trennung/Isolierung, gefordert.

¹ Die Arbeitsübersetzung der englischen Normentexte dient nur einer einfacheren Übersicht und erhebt nicht den Anspruch einer wortgetreuen Übersetzung. Bei Fragen der Interpretation von Aussagen wird empfohlen, auf den Originaltext zurückzugreifen.

– **Aufrechterhaltung der verfahrenstechnischen Redundanz und Diversität der Anlage**

Auch für Leitechniksysteme, die die gleiche sicherheitstechnische Bedeutung aufweisen, sind Anforderungen an die Unabhängigkeit vorgeschrieben, um die durch die Anlage zur Verfügung gestellte verfahrenstechnische Redundanz und Diversität im Fehlerfall nicht zu schwächen. Verbindungen von Systemen gleicher Kategorien müssen sicherstellen, dass die Unabhängigkeit untereinander aufrechterhalten bleibt, indem die Ausbreitung von Ausfällen verhindert wird. Für Kategorie A wird der Verzicht auf Verbindungen zwischen diversitären Leitechniksystemen gefordert. Weiterhin müssen für Kategorie A Vorrang- und Einzelantriebssteuerungen für die verfahrenstechnischen Redundanzen strangweise aufgebaut werden.

– **Leitechniksystemarchitektur**

Zur Erreichung der geforderten Zuverlässigkeit der einzelnen Leitechniksysteme ist auch für die Interfaces innerhalb eines Systems ein redundanter Aufbau vorzusehen, um die zugrunde zu legenden Fehlerarten und -kombinationen sowie die versagenauslösenden Ereignisse zu beherrschen. Ebenso darf die in der Systemarchitektur vorhandene Redundanz der Teilsysteme aufgrund von Vermaschungen durch die Interfaces nicht beeinträchtigt werden.

– **Unabhängigkeit von kommunizierenden Teilsystemen**

Für Verbindungen zwischen redundanten Teilsystemen wird die gegenseitige Unabhängigkeit gefordert, so dass versagenauslösende Ereignisse nicht den Ausfall mehrerer Redundanzen zur Folge haben. So ist u. a. durch Barrieren zur Fehlerausbreitung sicherzustellen, dass sich Ausfälle und Fehlverhalten in einer Redundanz nicht auf andere Redundanzen auswirken. Hierbei sind auch indirekte Verknüpfungen von Systemen über Service- oder Prüfgeräte zu berücksichtigen. Bestehen auch Verbindungen zwischen Systemen mit unterschiedlichen leittechnischen Funktionen, sind die Anforderungen an die Rückwirkungsfreiheit der Schnittstellen untereinander ebenfalls gefordert. Die Barrie-

ren zur Fehlerausbreitung sind hierbei einerseits elektrische Trennung sowie Schirmungs- und Erdungsmaßnahmen gegen elektromagnetische Beeinflussungen. Andererseits werden hierzu auch datentechnische Barrieren gefordert, die die Auswirkungen durch das Fehlverhalten eines Teilsystems auf damit verbundene Teilsysteme verhindern. Hierzu sind geeignete Kommunikationsarchitekturen und -protokolle einzusetzen.

– **Realisierung und Performance**

Zur Sicherstellung des vorherbestimmbaren Verhaltens der Leittechniksysteme wird insbesondere auch die Unabhängigkeit der Funktion der Interfaces von den zu übertragenden Daten sowie eine strikt zyklische Versendung der Daten gefordert. Durch die Datenverbindungen darf keine Synchronisation zwischen den unabhängigen Teilsystemen verursacht werden. Aufgrund der zeitlich verzögernden Wirkung von Datenkommunikationen muss die Einhaltung der spezifizierten Antwort- und Reaktionszeiten des Gesamtsystems unter allen zu unterstellenden Bedingungen garantiert werden können. Hierzu ist auch die vollständige Spezifikation und Dokumentation der unterschiedlichen Verhaltensweisen der Interfaces hinsichtlich Funktionalität und gerätetechnischer Eigenschaften gefordert.

– **Fehlererkennung und –beherrschung**

Es werden im Normenwerk sowohl Maßnahmen zur Fehlererkennung als auch zur Fehlerbeherrschung gefordert. Fehlerhafte Signale sind zu erkennen und in ihrer Ausbreitung einzugrenzen. Es ist eine regelmäßige Selbstüberwachung der Verbindungen vorzusehen. Das Ausfallverhalten muss vollständig offen gelegt sein und in den jeweiligen Anwendungen eine definierte Vorzugsrichtung im Fehlerfall einnehmen.

– **Security**

In den meisten Fällen erhöht der Einsatz von datentechnischen Verbindungen das Potenzial für unbefugte Manipulationen, da die datentechnischen Verbindungen zumeist den Fernzugriff auf die Systemkomponenten ermöglichen und auf der anderen Seite auf-

grund ihrer starken Verteilung in der Anlage nur schwer vollständig durch physische Maßnahmen geschützt werden können. Es wird daher die Analyse der Bedrohungen, die sich durch die Interfaces ergeben, sowie die Festlegung entsprechender wirksamer informationstechnischer Schutzmaßnahmen gefordert. Ziel ist es hierbei, den Zugriff auf die Software und die Daten der Leittechniksysteme zu beschränken und unbefugte Änderungen zu verhindern.

– **Kabel und Kabelverlegung**

Die Anforderungen an die Kabel und die Kabelverlegung, die auch für elektrische Einzelsignalleitungen gelten, gewinnt bei der Verwendung von Interfaces eine höhere Bedeutung, da aufgrund der Konzentration vieler Signale in einem Signalkabel ein Ausfall eine weit höhere Fehlerauswirkung aufweist. Weiterhin werden bei Busverbindungen teilweise aktive Netzwerkkomponenten im Kabelweg eingeschleift, für welche die Festigkeit gegen die Belastungen durch die Einsatzbedingungen ebenfalls gegeben sein muss. Die Kabel müssen für die unterstellten Umgebungsbedingungen ausgelegt sein, wobei auch eventuelle spezielle Belastungen, z. B. durch die Auslösung von Feuerbekämpfungssystemen, berücksichtigt werden sollen. Weiterhin sind physische Schutzmaßnahmen für die zu beherrschenden versagenauslösenden Ereignisse zu treffen. Es ist die physische Trennung zwischen redundanten Buskabeln und anderen Kabeltypen, die zu Beeinflussungen führen könnten (z. B. Kabel mit höherem Energieniveau), vorzusehen. Zusätzlich sind geeignete Abschirmungsmaßnahmen zur Sicherstellung der EMV zu treffen.

Die identifizierten Anforderungen im Einzelnen sind in Anhang III, gegliedert in die einzelnen Themengebiete, enthalten.

3.2 Anpassung des Fragenkatalogs aus dem Vorhaben SR 2422

Im Rahmen des Forschungsvorhabens SR 2422 /31/ wurde ein generischer Fragenkatalog für rechnergestützte periphere Komponenten erstellt, mit dem überprüft werden kann, ob bei der Entwicklung einer rechnergestützten Komponente die wesentlichen fehlerver-

meidenden und fehlerbeherrschenden Maßnahmen berücksichtigt wurden und ob für eine Begutachtung ausreichende Informationen und Unterlagen zur Verfügung gestellt werden können. Für rechnergestützte Interface-Baugruppen wurde der Fragenkatalog um spezifische Fragen ergänzt. Der neu hinzugefügte Abschnitt 9 „Spezielle Fragen zu Interface-Baugruppen“ beschäftigt sich mit speziell auf Kommunikationsinterfaces ausgerichtete Fragestellungen, die vom bisherigen Fragenkatalog aus dem Forschungsvorhaben SR 2422 nicht abgedeckt wurden. Folgende Fragen wurden ergänzt:

– **Busarchitektur**

- Welche Netztopologien sind möglich?
- Sind redundante Busstrukturen möglich?
- Ist ein Mischbetrieb mit nicht-sicherheitsgerichteten Nachrichten auf einer Kommunikationsverbindung möglich? Wie wird die gegenseitige Beeinflussung sicherheitsrelevanter und nicht sicherheitsrelevanter Nachrichten verhindert?

– **Hardware**

- Ist eine Übertragung über Lichtwellenleiter (LWL) möglich?
- Können konventionelle Netzwerkkomponenten für den Aufbau der Netztopologie verwendet werden?
- Welche Verbreitung hat die Komponente in der Industrie?

– **Protokoll**

- Welches Konzept liegt dem sicherheitsgerichteten Bussystem zugrunde?
- Welches Buszugriffsverfahren wird verwendet?
- Können die Nachrichten mit Prioritäten versehen werden?
- Ist die direkte Kommunikation von peripheren Busteilnehmern ohne Sicherheitszentrale möglich?



- Wie ist das Verhalten des Bussystems bezüglich der Reaktionszeit?
- Ist die der Baugruppe zugrunde liegende Protokollspezifikation herstellerspezifisch oder ein offen gelegtes Protokoll?
- Wie groß ist die Hamming-Distanz bei der Datenübertragung auf dem Bussystem?

– **Fehlerverhalten**

- Werden die typischen Fehler für Buskommunikation (Verlust, Wiederholung, Einfügung, falsche Abfolge, Verzögerung und Nachrichtenverfälschung) beherrscht? Welche Maßnahmen werden bei Fehlererkennung ergriffen?
- Wie wirkt sich der Ausfall einzelner Busteilnehmer auf das Netzwerk aus?
- Wird ein Watchdog verwendet?

4 Einführung in die Sicherheitsbustechnologie

In den letzten Jahren haben sich verstärkt sicherheitsgerichtete Varianten zu den am Markt etablierten Standardfeldbussen entwickelt. Sie zeichnen sich dadurch aus, dass sie auftretende Kommunikationsfehler sicher erkennen und eine entsprechende Fehlerkorrektur vornehmen oder entsprechende Fehlerreaktionen veranlassen können. Die Konzepte, auf welchem Weg diese Sicherheit erreicht wird, sind bei den Bussystemen jedoch unterschiedlich.

Die Entwicklung der Sicherheitsbussysteme orientiert sich meist an der Norm IEC 61508 /N11/ für allgemeine industrielle Sicherheitsanwendungen (siehe auch /34/ und /29/). In ihr werden Sicherheitsfunktionen entsprechend ihrer sicherheitstechnischen Bedeutung in Kategorien, sog. SIL-Level (Stufen 1 bis 4), eingeteilt. Zur Sicherstellung der Zuverlässigkeit der Sicherheitsfunktion fordert die IEC 61508 in Abhängigkeit vom zu erreichenden SIL-Level fehlerbeherrschende sowie fehlervermeidende Maßnahmen. Zur Sicherstellung der Zuverlässigkeit der Sicherheitsfunktion wird bei Erkennung eines Fehlers ein Fail-Safe-Verhalten durch den Übergang in einen definierten Fehlerzustand genutzt. Um die Wirksamkeit der fehlerbeherrschenden Maßnahmen zu überprüfen, muss die Sicherheitsfunktion einer Wahrscheinlichkeitsbetrachtung unterzogen werden. Dabei wird die sog. gefährliche Versagenswahrscheinlichkeit für nicht entdeckte Fehler, die zum Versagen der Sicherheitsfunktion führen, ermittelt. Diese muss unterhalb eines vom SIL-Level festgelegten Grenzwerts bleiben.

Eine grundsätzliche Voraussetzung beim Einsatz dieser Systeme stellt das Vorhandensein eines Fail-Safe-Zustandes dar, der als Reaktion auf erkannte Fehler ohne Beeinträchtigung der Sicherheit eingenommen werden kann. Für die Sicherheitsleittechnik in Kernkraftwerken muss hierzu im Einzelnen geprüft werden, ob und wie sich Komponenten mit diesem Verhalten unter Berücksichtigung der zu stellenden Zuverlässigkeitsanforderungen in das Leittechniksystem integrieren lassen.

4.1 Neue Fehlertypen im Zusammenhang mit Buskommunikation

Im Vergleich zu fest verdrahteten Systemen treten bei Systemen mit Busverbindungen neuartige Fehlertypen auf [29], die sich aus der paketorientierten Kommunikation in Bussystemen ergeben. Jedes Datentelegramm besteht aus einem Telegrammkopf (Header) und einem Nutzdatenanteil. Der Header enthält für den Kommunikationsablauf relevante Informationen, während der Nutzdatenanteil die zu übermittelnden Nutzdaten enthält. Eine Nachricht kann hierbei über mehrere Telegramme verteilt sein.

Folgende Fehlertypen sind hierbei zu unterscheiden:

- **Verlust**

Ein Verlust durch einen Fehler im Sender, Empfänger oder auf der Busverbindung bedeutet die komplette Löschung des Telegramms.

- **Wiederholung**

Eine Wiederholung liegt vor, wenn ein bereits gesendetes Telegramm zu einem späteren Zeitpunkt fälschlich wiederholt wird.

- **Einfügung**

Unter Einfügung versteht man die unbeabsichtigte Erweiterung der Nutzdaten eines Telegramms.

- **Falscher Ablauf**

Dieser Fehlertyp liegt vor, wenn die zeitliche Reihenfolge von Telegrammen durch einen Fehler so beeinflusst wird, dass eine ältere Nachricht nach einer zeitlich aktuelleren Nachricht beim Empfänger eintrifft.

- **Verzögerungen**

Durch Überlastung oder Fehler in der Busübertragung können Verzögerungen bei der Telegrammübermittlung entstehen.

– **Nachrichtenverfälschungen**

Nachrichtenverfälschungen können z. B. durch die Einwirkung von elektromagnetischen Störungen (EMV) auf die Übertragungsstrecke (Bus-Kabel) entstehen.

4.2 Konzept und Auslegung von Sicherheitsbussen

Gegen die in Kapitel 4.1 beschriebenen Fehlertypen der Datenkommunikation sind zur Erreichung des geforderten SIL-Levels Maßnahmen zur Fehlerbeherrschung zu ergreifen. In Standardfeldbussen sind derartige Vorkehrungen jedoch nur teilweise implementiert, so dass Sicherheitsbusvarianten auf der Basis von Standardfeldbussystemen entwickelt wurden. Hierbei lassen sich zwei verschiedene Ansätze unterscheiden: Das „Grey-Channel“-Prinzip und der Ausbau bestehender Sicherungsmechanismen, der in Analogie zum Grey-Channel nachfolgend als „White Channel“ bezeichnet wird /30/.

4.2.1 Grey-Channel

Sicherheitsbuskomponenten nach dem Grey-Channel-Prinzip setzen auf einem Standardfeldbussystem auf, wobei dessen Übertragungskanal unverändert genutzt wird. Da dieser Übertragungskanal als unsicher betrachtet wird, dient der Nutzdatenteil des Standardfeldbus-Telegramms lediglich als Transportmedium für das eingebettete sicherheitsgerichtete Telegramm, welches zusätzliche, eigenständige Sicherungsmechanismen aufweist. Die Sicherheitstelegramme werden damit durch den unsicheren Übertragungskanal getunnelt. Der Empfänger überprüft anhand der mitgelieferten Sicherungsinformationen, ob die Übertragung korrekt war und veranlasst gegebenenfalls den Übergang in den Fail-Safe-Zustand. Da die Sicherungsmechanismen im Protokoll verwirklicht und in das Telegramm eingebettet werden, ist dies ein softwarebasierter Ansatz (z. B. PROFIsafe, DeviceNET Safety).

Vorteil dieses Ansatzes ist, dass der in dezentralen Ein-/Ausgabebaugruppen verwendete Rückwandbus als Teil des unsicheren Kanals aufgefasst werden kann und in der Zertifizierung bzw. Begutachtung nicht zusätzlich betrachtet werden muss. Mit diesem Ansatz

ist weiterhin ein Mischbetrieb sicherheitsgerichteter und konventioneller Telegramme möglich. Die Standardbusteilnehmer ignorieren in diesem Fall die zusätzlichen Sicherungsinformationen, die für sie Nutzdaten darstellen. Ebenso ist die Verwendung von Standardindustriekomponenten für den Aufbau der Businfrastruktur möglich. Da die Sicherungsmechanismen im Protokoll verwirklicht werden, ist es leicht, diesen softwarebasierten Ansatz auf Fremdprodukte zu portieren. Beim Einsatz entsteht hinsichtlich der Busanschaltung kein zusätzlicher Hardwareaufwand im Vergleich zu Standardbusanschaltungen.

Die zusätzlichen Sicherungsinformationen bedingen im Gegenzug ein komplexeres Kommunikationsprotokoll und damit eine höhere Komplexität der Software. Der je Telegramm übertragbare Nutzdatenanteil sinkt im Vergleich zum Standardbussystem durch das Hinzufügen der Sicherungsinformation. Der geringere Nutzdatenanteil und der softwarebasierte Ansatz führen weiterhin zu Geschwindigkeitseinbußen im Vergleich zum Standardfeldbus.

4.2.2 Ausbau bestehender Sicherungsmechanismen (White-Channel)

Der Ausbau bestehender Sicherungsmechanismen, in Analogie zum Grey-Channel künftig White-Channel genannt, ist im Gegensatz zum Grey-Channel ein hardwarenaher Ansatz (z. B. CANopen Safety Chip, Esalan). Die Basis bildet ein Standardfeldbus, der bereits mit fehlerkorrigierenden Maßnahmen ausgestattet ist (z. B. Hamming-Distanz, Telegrammwiederholung). Die bereits geringe Wahrscheinlichkeit unerkannter Fehler des zugrunde liegenden Standardfeldbusses wird durch weitere Maßnahmen in der Treiber-Hardware, wie Wiederholung der Telegramme mit invertierten Daten auf redundanten Busanschaltungen, oder durch die Einführung zusätzlicher unabhängiger Überwachungskomponenten weiter reduziert. Die resultierende Fehlerrate gelangt so in einen Größenbereich, der für die sicherheitsgerichtete Kommunikation gemäß IEC 61508 anforderungsgerecht ist.

Beim Ausbau bestehender Sicherungsmechanismen müssen keine Sicherungsinformationen in das Telegramm eingebettet werden und der gesamte Nutzdatenanteil bleibt erhalten. Da die sichere Datenübertragung durch die Erweiterung bestehender Sicherungsmechanismen auf Hardwareebene erfolgt, können Übertragungsfehler teilweise korrigiert und die Verfügbarkeit verbessert werden. Auch in diesem Fall ist ein Mischbetrieb mit nicht sicherheitsgerichteten Nachrichten möglich, da das Busprotokoll selbst nicht verändert wird.

Im Gegensatz zum Grey-Channel-Ansatz können jedoch keine Standardkomponenten für die Buskommunikation verwendet werden, da das Übertragungsmedium nicht, wie beim Grey-Channel-Ansatz, unverändert beibehalten wird. Die spezielle Entwicklung von Hardwarekomponenten ist daher erforderlich.

4.3 Darstellung der unterschiedlichen Buszugriffsverfahren

Neben dem Konzept des Sicherheitsbusses beeinflusst auch das zugrunde liegende Standardfeldbussystem die Eigenschaften des Businterfaces /35/. Dazu zählen die möglichen Übertragungsraten und Leitungslängen, sowie das Buszugriffsverfahren. Im industriellen Bereich wird eine große Vielfalt von Buszugriffsverfahren eingesetzt. Abbildung 4 zeigt eine Übersicht der wichtigsten Verfahren. Grundsätzlich kann zwischen den Buszugriffsverfahren mit kontrolliertem und stochastischem Zugriff unterschieden werden.

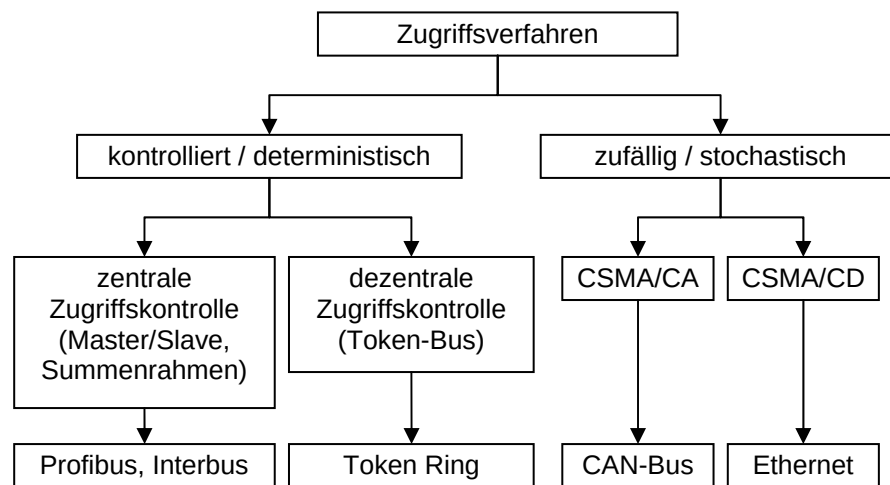


Abbildung 4: Übersicht der wichtigsten Buszugriffsverfahren

Beim kontrollierten Zugriffssystem ist der Ablauf der Buskommunikation fest vorgegeben. Ein Master hat die Oberhand über die Buskommunikation. Die Zuteilung des Busses erfolgt in gleichen Abständen in der vorgegebenen Reihenfolge an die Busteilnehmer, d. h. der Buszugriff ist zyklisch und deterministisch. Die Zuteilung kann hierbei zentral oder dezentral organisiert sein.

Bei zentral verwalteten Bussen mit Master/Slave-Verfahren (z. B. PROFIsafe) oder Summenrahmen-Verfahren (z. B. Interbus) gibt es einen Master, der den Busteilnehmern das Senderecht explizit erteilt. Dieses Verfahren ermöglicht einfache Businterfaces bei den Busteilnehmern, da die Intelligenz des Bussystems im Master konzentriert ist. Er teilt den Busteilnehmern nacheinander den Bus für eine definierte Zeit zu. Dazu sendet er ein Telegramm an einen der Busteilnehmer und fordert eine Nachricht bzw. eine Empfangsbestätigung von ihm. Die Busteilnehmer werden in fester Reihenfolge zyklisch nacheinander abgefragt. Fällt ein Busteilnehmer aus, so erkennt dies der Master und überspringt ihn beim nächsten Mal und der Bus kann ohne Einschränkung weiter betrieben werden. Das Buszugriffsverfahren ist prinzipiell echtzeitfähig, da jeder Busteilnehmer in festgelegter Weise Zugriff auf den Bus bekommt. Eine direkte Kommunikation zwischen den Busteilnehmern ist nicht möglich. Fällt der Master aus, kommt jedoch die gesamte Buskommunikation zum Erliegen.

Dezentrale Zugriffskontrollen arbeiten nach dem Token-Prinzip (z. B. Token-Ring). Dieses Vorgehen gleicht einem Staffellauf, bei dem das Token von einem Busteilnehmer zum nächsten weitergereicht wird. Nur der Busteilnehmer, der im Besitz des Tokens ist, hat das Senderecht. Ein Master bringt das Token in Umlauf und überwacht den Bus z. B. auf ein verloren gegangenes Token. Fällt ein Busteilnehmer aus, so schließt der Master ihn vom Token-Umlauf aus und der Bus kann weiter betrieben werden. Die maximale Token-Umlaufzeit ist bekannt und damit die maximale Reaktionszeit des Feldbussystems. Die einzelnen Busteilnehmer des Bussystems können direkt miteinander kommunizieren, sobald einer von beiden im Besitz des Tokens ist. Ändert sich die Teilnehmeranzahl, muss der Bus jedes Mal neu konfiguriert werden. Mit wachsender Teilnehmerzahl erhöht sich die maximale Token-Umlaufzeit.

Bei stochastischen Buszugriffsverfahren sind die Busteilnehmer zu jeder Zeit gleichberechtigt. Die Busteilnehmer legen ihre Telegramme ereignisgesteuert auf den Bus. Naturgemäß kann es dabei zu Kollisionen mit Telegrammen anderer Busteilnehmer kommen. In diesem Fall muss der Sendeversuch zumindest eines Busteilnehmers zu einem späteren Zeitpunkt wiederholt werden. Mit einer Erhöhung der Auslastung des Busses steigt die Wahrscheinlichkeit von Kollisionen. Das Buszugriffsverfahren ist damit vom zugrunde liegenden Prinzip her nicht deterministisch. Bei den stochastischen Buszugriffsverfahren wird zwischen dem CSMA/CD- und dem CSMA/CA-Verfahren unterschieden.

Das CSMA/CD-Verfahren (z. B. Ethernet) ist in der Lage, aufgetretene Kollisionen auf dem Bus zu erkennen. Beide Busteilnehmer brechen in diesem Fall ihre Übertragung ab. Nach einer zufällig gewählten Zeit versuchen es beide Busteilnehmer erneut. Bei diesem Verfahren können Busteilnehmer jederzeit hinzugefügt oder entfernt werden, ohne dass der Bus neu konfiguriert werden muss. Greifen allerdings zu viele Busteilnehmer auf den Bus zu, sinkt die Effizienz des Buszugriffsverfahrens erheblich. Da die Kollisionen nicht vorhersagbar sind und die Zeitspanne zwischen einer Telegrammkollision und der erneuten Sendung der Telegramme zufällig ist, können die maximalen Signalzeiten nur geschätzt werden.

Im Unterschied zum CSMA/CD-Verfahren arbeitet das CSMA/CA-Verfahren (z. B. CAN-Bus) auf Basis der Kollisionsvermeidung. Wollen mehrere Busteilnehmer zufällig zum gleichen Zeitpunkt senden, erfolgt zu Beginn mit dem parallelen, synchronen Senden der Telegrammheader ein Vergleich der Prioritäten der Telegramme. Die Priorität ist von dem absendenden Busteilnehmer abhängig und erlaubt eine eindeutige Rangfolge der Telegramme. Bei diesem als Arbitrierung bezeichneten Vorgang setzt sich letztendlich das Telegramm mit der höchsten Priorität durch und seine Übermittlung bleibt ungestört. Die unterlegenen Busteilnehmer beginnen anschließend einen erneuten Sendeversuch. Die Kommunikation läuft demnach zwar ereignisgesteuert ab, aber die einzelnen Busteilnehmer können mittels Prioritäten hinsichtlich ihrer Bedeutung gewichtet werden.

5 Beschreibung der Typvertreter

Im Rahmen des Vorhabens SR 2422 wurden die Anforderungen, die an rechnergestützte periphere Komponenten des Sicherheitssystems in Kernkraftwerken zu stellen sind, untersucht. Unter rechnergestützten peripheren Komponenten sind Komponenten zu verstehen, die abgesetzt von den Zentraleinrichtungen eingesetzt werden und mit Mikrocontrollern, Mikroprozessoren oder anderen hochintegrierten Bauteilen ausgerüstet sind. Es wurde ein generischer Fragenkatalog aufgestellt und dieser für mehrere Typvertreter im Bereich der Messwerterfassung, der Antriebssteuerung und der elektrischen Energieversorgung des Sicherheitssystems von Kernkraftwerken beantwortet. Zur Ergänzung des Forschungsvorhabens SR 2422 wurde im vorliegenden Forschungsvorhaben SR 2499 für zwei Typvertreter von Interfacebaugruppen ein entsprechend angepasster Fragenkatalog (vgl. Kapitel 3.2) beantwortet.

5.1 Marktrecherche und Auswahlkriterien

Die Eignung der am Markt erhältlichen Sicherheitsbussysteme soll exemplarisch anhand zweier Typvertreter untersucht werden. Zur Auswahl der Typvertreter wurde eine Marktrecherche der in der Industrie verwendeten Sicherheitsbussysteme durchgeführt. Tabelle 1 zeigt eine Zusammenfassung der wichtigsten zurzeit am Markt vertretenen Sicherheitsbussysteme. Die farbliche Markierung kennzeichnet das zugrunde liegende Buszugriffsverfahren:

- gelb: Pollingverfahren (Master/Slave)
- weiß: Master/Slave-Verfahren mit Sicherheitsmonitor
- rot: Summenrahmen
- grün: CAN (CSMA/CA)
- blau: Ethernet (CSMA/CD)

Das Token-Prinzip ist aufgrund seiner geringen Marktrelevanz nicht vertreten.

Wichtige Kriterien für die Auswahl der Typvertreter waren deren abgeschlossene Zertifizierung sowie die Verfügbarkeit des zugehörigen Prüfberichts nach IEC 61508 und eventuell ergänzender Entwicklungsdokumentation bzw. Produktbeschreibungen. Neben diesen grundsätzlichen Forderungen sollen die Typvertreter das in Tabelle 1 aufgeführte Spektrum industrieller Sicherheitsbussysteme möglichst breit abdecken, d. h. die Typvertreter sollten auf unterschiedlichen Standardbussystemen aufbauen und jeweils Vertreter eines der beiden Sicherheitsbuskonzepte White- und Grey-Channel sein. Die Marktrelevanz des Systems bzw. ob die Gerätetechnik bereits in der Kerntechnik eingesetzt ist, wurden bei der Typvertreterauswahl ebenfalls berücksichtigt.

Bus	Topologie	Bemerkungen	Zertifizierung	Einführung	Medium	Hersteller
PROFIsafe	Linienförmig (zentral: Ringförmig)	Monomaster Pollingverfahren (zentral: Multimaster Token)	IEC 61508 SIL 3 (TÜV Süd) DIN 19250 AK 6 EN 954-1 Kategorie 4	2002	CU, LWL	PNO offen
AS-Interface Safety at Work	Linien-, Stern- und Baumförmig	Monomaster Pollingverfahren Sicherheitsmonitor (keine Sicherheits-SPS erforderlich)	IEC 61508 SIL 3 (TÜV Rheinland) EN 954-1 Kategorie 4 (TÜV Nord)	2000	CU	Siemens
Interbus Safety	Ringförmig (von außen gesehen Linienstruktur)	Monomaster Summenrahmen Überwachungseinheit „Safe-Control“ nur für einfache E/A-Geräte	EN 954-1 Kategorie 4 (BIA)	1987	CU, LWL	Phoenix DIN E 19258
SafetyBUS p	Linienförmig (Stern- und Baumstrukturen mit Netzstrukturelementen)	basiert auf CAN Master/Slave Pollingverfahren Multimasterfähig	IEC 61508 SIL 3 (TÜV Süd) u. U. SIL 4 DIN 19250 AK 6 (TÜV Süd) EN 954-1 Kategorie 4	1999	CU, LWL	Pilz offen
DeviceNET Safety	Linienförmig, Stichleitungen	basiert auf CAN CIP Multimasterfähig direkte Kommunikation möglich (ohne Master)	IEC 61508 SIL 3 (TÜV Rheinland)	2005	CU	ODVA offen
CANopen Safety Chip	Linienförmig	CSMA/CA Busarbitrierung White-Channel-Prinzip Multimasterfähig direkte Kommunikation möglich (ohne Master)	IEC 61508 SIL 3 (TÜV Rheinland)	2004	CU, LWL	CAN in Automation
Esalan	Linienförmig	basiert auf CAN Multimasterfähig direkte Kommunikation möglich (ohne Master)	DIN 19250 AK 6 EN 954-1 Kategorie 4 (BIA)		CU, LWL	Elan proprietär
EPLSafety	Linien-/Baumförmig	basiert auf Ethernet-Hardware Safety-Frame CAN entlehnt direkte Kommunikation möglich (ohne Master)	IEC 61508 SIL 3 (TÜV Rheinland) u. U. SIL 4 (nicht abgeschlossen)	2005	CU, LWL	Innotec, B&R, ...
SaveEthernet	Sternförmig	basiert auf Ethernet	IEC 61508 SIL 3 (TÜV Rheinland) EN 954-1 Kategorie 4 (TÜV Rheinland)	1997	CU, LWL	HIMA proprietär

Tabelle 1: Zusammenstellung der wichtigsten Sicherheitsbussysteme

– **PROFIsafe**

PROFIsafe wurde von der PROFIBUS-Nutzerorganisation (PNO) veröffentlicht und zählt zu den offen gelegten Protokollen unter den Sicherheitsbussen /21/. Das System wurde durch den TÜV SÜD nach IEC 61508 zertifiziert. Es erlaubt die rückwirkungsfreie Koexistenz der Sicherheitskommunikation und der Standardkommunikation auf ein- und demselben Bus. Die Sicherheitskommunikation arbeitet nach dem Grey-Channel-Prinzip. Die Bustopologie wird linienförmig aufgebaut. Die Sicherheitszentrale fragt die Busteilnehmer nacheinander mit einem Pollingverfahren ab. Zwischen mehreren Sicherheitszentralen erfolgt die Vernetzung ringförmig über eine multimasterfähige Token-Kommunikation.

– **AS-Interface Safety at Work**

AS-Interface Safety at Work /27/ wurde von einem Konsortium (u. a. Siemens, Schneider Electric, Festo) primär für die Vernetzung binärer Sensoren und Aktoren entwickelt und ist durch den TÜV Rheinland nach IEC 61508 SIL3 sowie durch den TÜV Nord bis Kategorie 4 nach EN 954-1 /N15/ zertifiziert. Bei AS-Interface Safety at Work wird zum Erreichen der geforderten Sicherheit der sog. Sicherheitsmonitor zusätzlich in den Bus eingebracht (White-Channel-Prinzip). Der Sicherheitsmonitor greift nicht in den Datenverkehr zwischen Master und Slaves ein, sondern überwacht lediglich die Kommunikation und leitet daraus den Schaltzustand jedes einzelnen sicherheitsgerichteten Slaves ab. Am Standard-Kommunikationssystem werden keinerlei Änderungen vorgenommen, wodurch ein Mischbetrieb mit betriebsmäßigen Funktionen möglich ist. Über die linien-, stern-, oder baumförmige Busverkabelung werden gleichzeitig die Informationen und die Energieversorgung der Aktoren und Sensoren geführt.

– **Interbus Safety**

Die drei Unternehmen innotec, Phoenix und Sick haben gemeinsam den sicherheitsgerichteten Feldbus Interbus Safety entwickelt /28/. Der Aufbau des Standardbussystems bleibt bei diesem Sicherheitsbussystem unverändert. Für das Erreichen der geforderten Sicherheit werden keine Protokolländerungen vorgenommen, sondern es werden eine

oder mehrere Zusatzkomponenten in den Bus integriert, welche die Sicherheit des Systems überwachen und im Fehlerfall geeignet reagieren (White-Channel-Prinzip). Diese Zusatzkomponenten arbeiten eigenständig, überwachen sich aber auch gegenseitig. Eine Zertifizierung gemäß EN 954-1 bis Kategorie 4 wurde von dem Berufsgenossenschaftlichen Institut für Arbeitssicherheit (BIA) durchgeführt, eine Zertifizierung gemäß IEC 61508 existiert nicht. Die Netzstruktur ist ringförmig, da das Protokoll auf Basis der Summenrahmen-Technik arbeitet, bei der ein Datenframe zirkulär durch alle Busteilnehmer gereicht wird.

– **SafetyBUS p**

SafetyBUS p wurde von der Firma Pilz speziell für den sicherheitstechnischen Einsatz entwickelt /21/. Die offene Sicherheitsbuslösung wird durch die Nutzerorganisation „SafetyBUS p Club International e. V.“ vertreten. Das System wurde durch den TÜV Süd nach IEC 61508 zertifiziert. Die Buskommunikation basiert auf dem CAN-Protokoll, die Topologie ist linienförmig. Die Realisierung der Sicherungsmechanismen erfolgt auf Protokollebene (Grey-Channel-Prinzip). Ein mehrkanaliger Aufbau des Busses für sicherheitsgerichtete Aufgaben ist vorgesehen. Das verwendete Master/Slave-Verfahren ist multimas-terfähig, d. h. mehrere Zentralen können zusammen auf die Peripherie zugreifen.

– **DeviceNET Safety**

DeviceNET Safety ist eine offene Netzwerkprotokollspezifikation, die von der ODVA (Open DeviceNet Vendors Association) gepflegt wird /23/. Das System ist noch nicht zertifiziert, es liegt allerdings eine positive Konzeptbeurteilung durch den TÜV Rheinland vor. Das DeviceNET-Netzwerk basiert auf dem CAN-Bus und arbeitet nach dem Producer/Consumer-Netzwerkmodell. Im Producer/Consumer-Netzwerkmodell sind die Telegrammdaten für alle Systemkomponenten gleichzeitig verfügbar. Mit diesem Netzwerkmodell wird die direkte Kommunikation der Systemteilnehmer ermöglicht. Auf Basis des Standardbussystems DeviceNet werden für den sicherheitsgerichteten Betrieb Sicherungsinformationen in einer zusätzlichen Sicherungsebene hinzugefügt (Grey-Channel-

Prinzip). Die Netztopologie ist linienförmig mit Stichleitungen zu den einzelnen Busteilnehmern.

– **CANopen Safety Protokoll**

Das offen gelegte CANopen Safety Protokoll wird von der Nutzerorganisation „CAN in Automation“ (CiA) vertreten /12/. Es setzt zum Erreichen des geforderten Sicherheitslevels auf eine Hardwareredundanz mit Kreuzvergleich (White-Channel-Prinzip). Der CANopen Safety Chip integriert diese Funktionalität in einem Chip und ist vom TÜV Rheinland gemäß IEC 61508 zertifiziert. Das im CAN-Controllerchip implementierte Protokoll enthält ein CRC-Verfahren zur Fehlererkennung. Zusätzliche Sicherheit ergibt sich durch die redundante Telegrammübermittlung mit Kreuzvergleich. Die Netztopologie ist linienförmig.

– **Esalan**

Esalan (Elan Safety Local Area Network) ist eine proprietäre (firmenspezifische) Lösung der Firma Elan /24/. Eine Zertifizierung gemäß EN 954-1 /N15/ Kategorie 4 erfolgt durch das BIA. Auch dieses Sicherheitsbussystem basiert auf dem CAN-Protokoll. Obwohl ausgewählte Standard-CAN-Komponenten zum Einsatz kommen, liegt das Ziel der proprietären Lösung in der hohen Echtzeitfähigkeit mit einer maximalen Reaktionszeit von 15 ms, auch im Fehlerfall. Die Busteilnehmer sind inklusive Mikrocontroller und CAN-Interface redundant aufgebaut und führen einen Kreuzvergleich der übertragenen Daten durch (White-Channel-Prinzip). Innerhalb der linienförmigen Netztopologie ist auch die direkte Kommunikation zwischen Busteilnehmern möglich.

– **EPLSafety und SaveEthernet**

Die beiden Sicherheitsfeldbussysteme EPLSafety /25/ und SaveEthernet /26/ basieren auf dem Kommunikationsprotokoll Ethernet. EPLSafety (Ethernet Powerlink Safety) ist ein offenes Protokoll der EPSG (Ethernet Powerlink Standardization Group), SaveEthernet ein proprietäres Sicherheitsbussystem der Firma HIMA. Beide arbeiten nach dem

Grey-Channel-Prinzip. Für EPLSafety ist die Zertifizierung durch den TÜV Rheinland noch nicht abgeschlossen, während SaveEthernet vom TÜV Rheinland bereits nach IEC 61508 SIL3 zertifiziert ist. Die Prüfberichte sind jedoch nicht offen gelegt. Für den Netzaufbau stehen die bei Ethernet-Netzwerken üblichen Strukturelemente wie Hubs oder Switches zur Verfügung. Mit ihrer Hilfe können sternförmige bzw. baumförmige Netze aufgebaut werden. Durch die Verwendung von FastEthernet Komponenten sind die Erreichung einer hohen Performance und der Mischbetrieb mit nicht sicherheitsgerichteter Kommunikation möglich.

5.2 Typvertreter I: PROFIsafe Profil

Der Typvertreter I repräsentiert das Sicherheitskonzept Grey-Channel. PROFIsafe /21/ gehört zur Gruppe der kontrollierten Zugriffsverfahren mit zentraler Zugriffskontrolle (Master/Slave-Verfahren). Da PROFIsafe zusammen mit der Zentralentechnik SIMATIC S7 F/FH der Firma Siemens AG angeboten wird, die bereits als Steuerung in kerntechnischen Anlagen eingesetzt ist, hat sich die Auswahl dieses Typvertreters besonders angeboten.

5.2.1 Beschreibung

PROFIsafe basiert auf dem Standardindriebussystem PROFIBUS DP. Grundlage für die Entwicklung von PROFIsafe waren einschlägige Standards, allen voran die IEC 61508. Die in Kapitel 4.1 aufgelisteten Fehlertypen werden durch folgende Maßnahmen beherrscht:

- fortlaufende Nummerierung der Sicherheitstelegramme
- Zeiterwartung für ankommende Telegramme und deren Quittierung
- Kennung zwischen Sender und Empfänger („Lösungswort“)
- zusätzliche Datensicherung (CRC)

Diese Maßnahmen werden in einer Softwareschicht oberhalb der DP-Layer-Schicht implementiert (siehe Abbildung 5). Der Standard-PROFIBUS dient als Transportmedium (Tunnel) für die sicherheitsgerichteten Nachrichten. Dieses Vorgehen erlaubt einen Mischbetrieb von Standard- und sicherheitsgerichteten Komponenten.

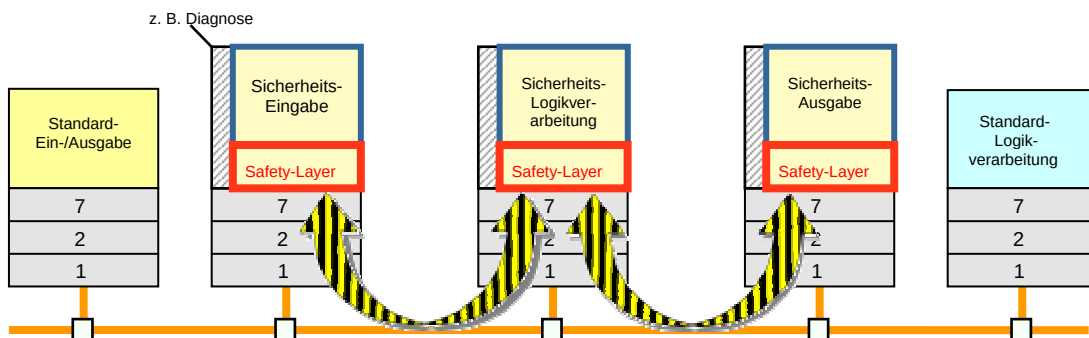


Abbildung 5: ISO/OSI Schichtenmodell von PROFIsafe

Als fertige Automatisierungssysteme, die PROFIsafe für die Buskommunikation zwischen Zentraleinheit und Ein-/Ausgabebaugruppen einsetzen, werden von der Firma Siemens

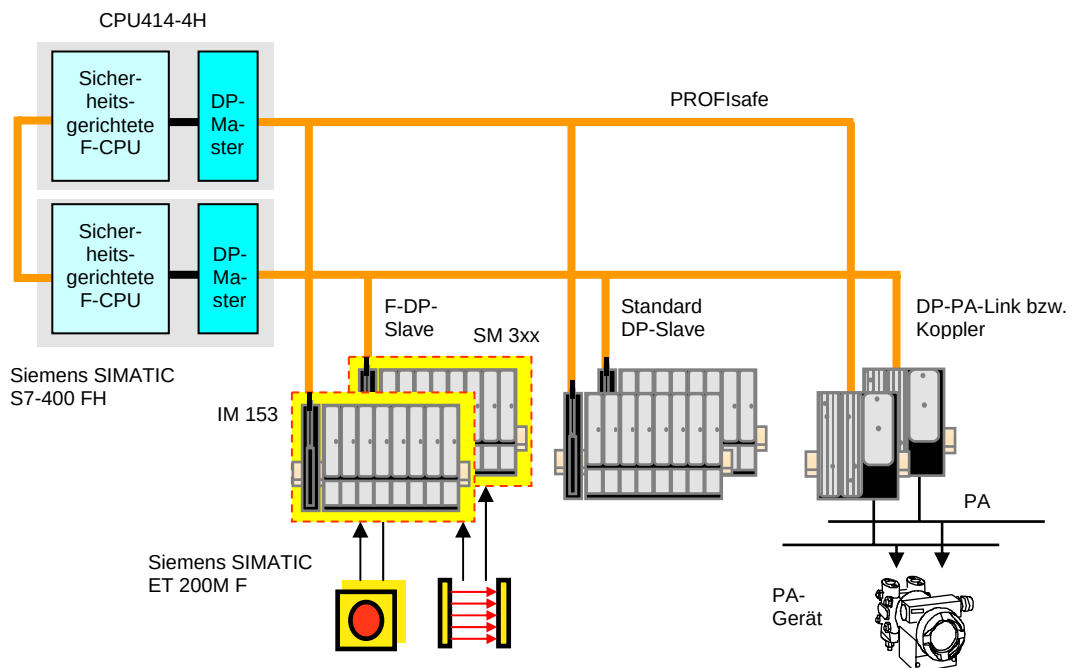


Abbildung 6: Systemaufbau SIMATIC S7 FH

AG die beiden Systeme SIMATIC S7 Distributed Safety und SIMATIC S7 F/FH Systems angeboten. Während das System SIMATIC S7 Distributed Safety den Mischbetrieb betrieblicher und sicherheitsgerichteter Anwendungen auf einem gemeinsamen Bus zulässt, wird SIMATIC S7 F/FH Systems für reine Sicherheitsfunktionen eingesetzt. In der Ausführung FH wird das System zur Erhöhung der Verfügbarkeit redundant aufgebaut (Abbildung 6).

Die Ein-/Ausgabebaugruppen werden über einen Rückwandbus zur sog. „dezentralen Peripherie“ zusammengefasst (ET 200M). Die fehlersicheren Ein-/Ausgabebaugruppen sind mit zwei redundanten Mikrocontrollern ausgestattet, die sich gegenseitig überwachen. Mit der Buskoppelbaugruppe IM 153 erfolgt die Anbindung an die Zentrale über PROFIsafe. Die Zentrale besteht aus einer sicherheitsgerichteten CPU, auf der das Automatisierungsprogramm abläuft, und einem DP-Master als Buskoppler. Sowohl Master, dezentrale Peripherie als auch die Busverbindung können redundant aufgebaut werden.

Der PROFIsafe arbeitet mit einem Master/Slave-Verfahren nach dem Polling-Prinzip. Die Zentrale (Master) fragt die Busteilnehmer (Slaves) in festgelegter Reihenfolge zyklisch nacheinander ab. Eine direkte Sensor-Aktor Kommunikation ist aufgrund der zentralen-basierten Kommunikationsstruktur nicht möglich. Die Verwaltung des Bussystems obliegt der Zentrale. Die Identifizierung der Busteilnehmer erfolgt anhand der konfigurierbaren Busadressen der Busteilnehmer. Da der Ablauf der Busteilnehmerabfrage bekannt ist, lässt sich die Reaktionszeit im fehlerfreien Fall exakt berechnen (Echtzeitfähigkeit). Für den Fehlerfall können Worst-Case-Abschätzungen vorgenommen werden. Im Extremfall entspricht die Fehlererkennungszeit einem kompletten Abfrageumlauf, da der Ausfall eines Busteilnehmers bei Polling-Betrieb spätestens bei der nächsten Abfrage sicher erkannt wird. Der Ausfall der Zentrale bedeutet jedoch den vollständigen Ausfall der Buskommunikation. In diesem Fall erkennen die Busteilnehmer den Ausfall des Busses und wechseln in den als solchen definierten Fail-Safe-Zustand.

5.2.2 Umfang und Ergebnis der Typprüfung

Zertifikate und Prüfberichte nach IEC 61508 liegen einerseits für die Software des PROFIsafe-Treibers /1/ von der TÜV Product Service GmbH TÜV Süd Gruppe vor. Andererseits liegen Prüfberichte für die Systeme SIMATIC S7 Distributed Safety /2/, /3/ und SIMATIC S7 F/FH Systems /4/, /5/ von der TÜV Automotive GmbH TÜV Süd Gruppe vor, die die einzelnen Komponenten der Automatisierungssysteme abdecken. Dazu zählen im Fall des SIMATIC S7 FH Systems die zentrale Baugruppe (F-CPU und DP-Master), die Buskoppler IM der dezentralen Peripherie und die Ein-/Ausgabemodule F-SM. Außerdem ist der Stand typgeprüfter fehlersicherer Programmbausteine für das sicherheitsgerichtete Automatisierungsprogramm festgehalten.

Ergebnis der Typprüfungen des PROFIsafe Treibers und der SIMATIC S7 Systeme ist die Erfüllung der Testkriterien und geforderten Qualitätsmerkmale der DIN V 19250 /N16/ für Kategorie AK 6, der EN 954-1 /N15/ Kategorie 4 und der IEC 61508 /N11/ SIL3. Ebenfalls erfüllt werden die Normen 93/68/EEC /N17/, DIN V VDE 0801 /N14/, prEN 50159-1 /N18/, VDI/VDE 2180 /N19/, DIN VDE 0116 /N20/, EN 298 /N21/, EN 61131-2 /N22/ und EN 60204-1 /N23/. Die Entwicklung erfolgte unter Anwendung von Qualitätssicherungsmaßnahmen nach DIN EN ISO 9001:2000. Die auslegungsspezifischen Reaktionszeiten müssen für spezifische Applikationen im Zusammenhang mit der gesamten Hardware ermittelt werden.

5.2.3 Auswertung des Fragenkataloges

Die Firma Siemens AG besitzt hinsichtlich des Qualitätsmanagements ein allgemeines Kontroll- und Qualitätsmanagementsystem nach DIN EN ISO 9001:2000. Das produkt-spezifische Qualitätsmanagement für Herstellung/Entwicklung und Produktprüfung sowie die Entwicklungsunterlagen wurden im Rahmen der Typprüfung geprüft. Nähere Einzelheiten hierzu wurden im Rahmen eines Interviews mit Siemens A&D dargelegt. Hinsichtlich Details zur Entwicklung wurde auf die Spezifikation des PROFIsafe-Treibers /7/ und

die Produktbeschreibungen /8/ – /11/, /21/ sowie die in dem Interview mitgeteilten Informationen zurückgegriffen.

Die Funktionen und Auslegungsvorgaben unter Sicherheitsaspekten resultieren aus der Qualifizierungsfähigkeit gemäß IEC 61508 SIL3. Die analytischen Maßnahmen zur Fehlervermeidung bei der Entwicklung wurden im Rahmen der Zertifizierung überprüft. Geeignete analytische Maßnahmen zur Fehlervermeidung bei der Entwicklung konnten anhand des im Interview dargelegten Prüfvorgehens nachvollzogen werden. Der Systemaufbau sowie der Hardware- und Softwareaufbau sind gemäß den Angaben des Herstellers detailliert beschrieben und lassen konstruktive Maßnahmen zur Fehlervermeidung bei der Hard- und Softwareentwicklung erkennen. Anforderungen an konstruktive Maßnahmen zur Fehlervermeidung bei der Softwareentwicklung resultieren aus der Qualifizierungsfähigkeit gemäß IEC 61508 SIL3. Die Programmlaufzeiten sind deterministisch und der Programmablauf ist streng zyklisch. Die Maßnahmen zur Fehlererkennung und Fehlerbeherrschung basieren auf der softwarebasierten Fehlererkennung der Buskommunikation gemäß dem Grey-Channel-Prinzip. Die Siemens S7 Systeme stellen parametrierbare Überwachungszeiten und einen Watchdog bereit.

Zusammenfassend kann festgestellt werden, dass der Typvertreter I PROFIsafe die Anforderungen der IEC 61508 SIL3 für eine sicherheitsgerichtete Kommunikation erfüllt. Automatisierungssysteme, die PROFIsafe für die Buskommunikation zu den Ein-/Ausgabebaugruppen einsetzen, werden von der Firma Siemens AG mit den beiden Systemen SIMATIC S7 Distributed Safety und SIMATIC S7 F/FH Systems angeboten, die ebenfalls nach IEC 61508 SIL3 zertifiziert wurden. Die anhand des Fragenkatalogs zusammengestellten Informationen auf der Basis der verfügbaren Unterlagen und der im Interview mitgeteilten Informationen haben keine grundsätzlichen Anhaltspunkte gegen den Einsatz in kerntechnischen Leitechniksystemen, die Sicherheitsfunktionen der Kategorien A und B ausführen, ergeben. Für den Einsatz in kerntechnischen Anlagen wären aber noch ergänzende Unterlagen sowie Nachweise, die die einzelnen Angaben belegen, erforderlich.

5.3 Typvertreter II: CANopen Safety Chip

Als Vertreter für das Konzept des White-Channels (Ausbau bestehender Sicherungsmaßnahmen) wurde der CANopen Safety Chip ausgewählt. Dieser zweite Typvertreter basiert auf dem CAN-Bus, der zu den stochastischen Bussystemen zählt. Das zugrunde liegende CANopen Profil ist im industriellen Bereich weit verbreitet. Obwohl die Entwicklung und Zertifizierung dieser sicherheitsgerichteten CANopen-Variante erst vor kurzem zum Abschluss gekommen ist, besitzt sie großes Potential, sich in Zukunft am Markt zu etablieren.

5.3.1 Beschreibung

Die sicherheitsgerichtete Version des CAN-Busses setzt auf der CANopen-Safety-Spezifikation auf. Diese Protokoll-Spezifikation wird von der Nutzerorganisation „CAN in Automation“ (CiA) standardisiert und weiterentwickelt. Die Spezifikation definiert ein firmenübergreifendes, offenes Protokoll, mit dem der Datenaustausch herstellerunabhängig festgelegt wird. Die sicherheitsgerichtete Version des CANopen Profils sieht folgende ergänzende Maßnahmen zur Beherrschung der in Kapitel 4.1 beschriebenen Fehlertypen vor:

- zeitversetztes Senden invertierter CAN-Telegramme über redundante CAN-Controller mit Kreuzvergleich beim Empfänger
- fortlaufende Nummerierung der Sicherheitstelegramme
- Zeiterwartung für ankommende Telegramme und deren Quittierung
- Prüfung bezüglich der Reihenfolge und der Priorität der CAN-Identifizier

Im Gegensatz zu dem rein softwarebasierten Ansatz des PROFIsafe wird bei der sicherheitsgerichteten Variante des CANopen Profils ein hardwarenaher Ansatz verfolgt. Die zusätzlichen Sicherungsmaßnahmen werden mit dem CANopen Safety Chip (CSC01) zur Verfügung gestellt. Abbildung 7 zeigt den prinzipiellen Aufbau des CSC01 und dessen

Einbindung in das Kommunikationsnetzwerk. Die Übermittlung der CANopen Telegramme erfolgt über zwei redundante CAN-Controller. Diese legen zeitversetzt und bitweise invertiert das gleiche Telegramm über denselben CAN-Treiber auf den BUS. Der Empfänger, der ebenfalls über zwei redundante CAN-Controller einliest, führt einen Kreuzvergleich der redundanten Telegramme durch. Die Fehlererkennungsmechanismen Nummerierung, Zeiterwartung, Quittierung, usw. werden fest in den Mikrocontroller einprogrammiert.

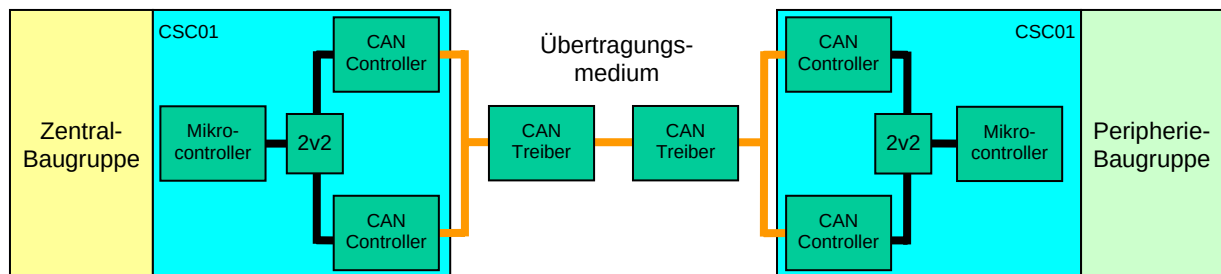


Abbildung 7: Prinzipschaltbild des CANopen Safety Chips

Mit diesem Typvertreter steht kein komplettes Automatisierungssystem zur Verfügung, wie es beim PROFIsafe mit SIMATIC S7 F/FH Systems oder SIMATIC Distributed Safety der Fall ist. Der betrachtete Chip umfasst ausschließlich das Kommunikationsinterface zwischen Bus und Applikation. Der CSC01 kann als fertiger Baustein von Geräteherstellern als Businterface eingebaut werden.

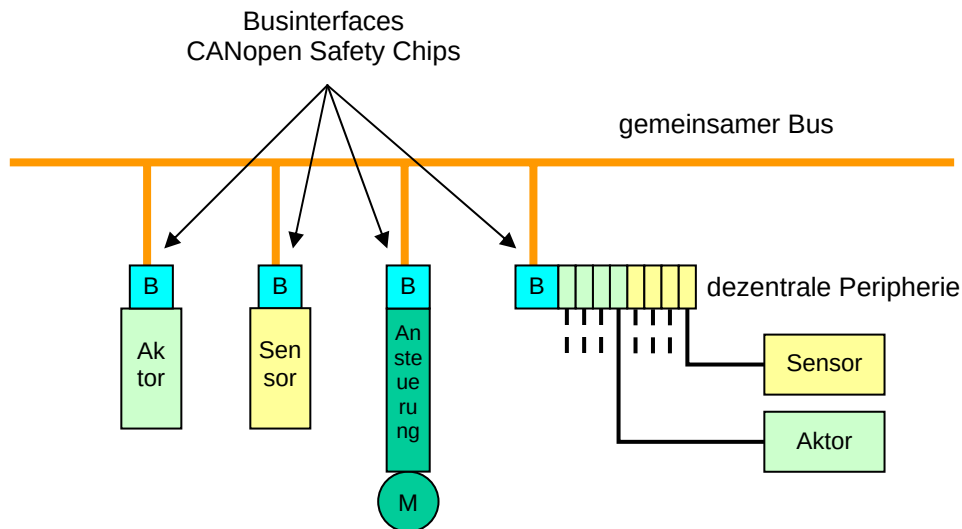


Abbildung 8: Systemaufbau CANopen Safety Bus

Abbildung 8 zeigt den prinzipiellen Aufbau eines CAN-Netzwerkes. Bei Standard-CAN greifen alle Busteilnehmer auf einen gemeinsamen Bus zu und können zu beliebigen Zeitpunkten Telegramme absetzen. Damit ist die Beherrschung von Kollisionen notwendig. Die Auswahl des Sendeberechtigten für diese Fälle erfolgt auf Protokollebene. Dieser Vorgang wird Arbitrierung genannt. Eine Zentrale ist bei dem Buszugriffsverfahren daher nicht zwingend notwendig und die direkte Kommunikation zwischen den Busteilnehmern ist möglich.

Die Telegramme enthalten keine Empfangsadresse, sondern eine Absenderadresse, den sog. Identifier. Jeder Busteilnehmer hört auf dem Bus mit und entscheidet anhand des Identifiers, ob das Telegramm für ihn bestimmt ist. Damit ist auch das Senden von Broadcast-Nachrichten an mehrere Empfänger möglich. Die Zuteilung des Senderechts bei Kollisionen erfolgt ebenfalls über den Identifier, über den gleichzeitig die Priorität der Nachricht festgelegt ist. Senden mehrere Busteilnehmer zur selben Zeit auf dem Bus, so werden die Identifier verglichen. Sobald ein Busteilnehmer den Sendewunsch eines Busteilnehmers mit höherer Priorität erkennt, zieht er seinen Sendewunsch zurück und versucht es später erneut. Die Zerstörung von Telegrammen wird somit verhindert und die Übertragung von hochprioritären Nachrichten bevorzugt behandelt. Eine Kommunikation ist

prinzipiell auch nach Ausfall einer eventuell vorhandenen Zentrale möglich. Der Ausfall eines Busteilnehmers wird jedoch ohne zusätzliche Überwachungsmechanismen von der Zentrale nicht automatisch erkannt.

Das CANopen Safety Protokoll ist ebenso wie das zugrunde liegende CAN-Protokoll prinzipiell ereignisgesteuert und arbeitet mit Prioritäten für die einzelnen Telegramme. Im Gegensatz zum CAN-Bus als stochastisches Bussystem implementiert der CANopen Safety Bus jedoch ein deterministisches Zugriffsverhalten, da im Protokoll Techniken für eine zyklische Datenübertragung implementiert wurden. Bereits im CAN-Standard sind weit reichende Maßnahmen zur Fehlererkennung und Korrektur enthalten. EingangsfILTER in den Businterfaces der einzelnen Busteilnehmer erlauben die Filterung veralteter Daten. Da das CANopen Safety Protokoll nicht masterbasiert ist, gefährdet der Ausfall einzelner Busteilnehmer die Funktion des Busses nicht.

5.3.2 Umfang und Ergebnis der Typprüfung

Gegenstand der Typprüfung war ein teilweise vorprogrammierter 16-Bit Mikrocontroller mit zwei redundanten CAN-Controllern. Die Software des CANopen Safety Chips besteht immer aus zwei Teilen, der permanenten Firmware und einem Applikationsprogramm. Die permanente Firmware enthält die Umsetzung des CANopen Safety Protokolls und zusätzlicher Diagnosefunktionen. Das Applikationsprogramm wird vom Gerätehersteller geliefert und ist nicht Teil der Typprüfung.

Der CANopen Safety Chip CSC01 erfüllt die Anforderungen für SIL3 gemäß IEC 61508 /6/ und kann in Anwendungen bis Sicherheitskategorie 4 nach EN 954-1 eingesetzt werden. Als Randbedingung der Zertifizierung wurde festgelegt, dass wenn der CSC01 in einem Gerät mit Aktorfunktionalität verwendet wird, ein Watchdog mit zweitem Abschaltweg vom Applikationshersteller realisiert werden muss.

5.3.3 Auswertung des Fragenkataloges

Die Firma SYSTEC electronic GmbH besitzt ein allgemeines Kontroll- und Qualitätsmanagementsystem nach DIN EN ISO 9001:2000. Der Entwicklung lagen interne Arbeitsanweisungen zugrunde. Eine ausführliche Entwicklungsdokumentation lag vor /13/ – /18/. Diese wurde vom TÜV Rheinland im Zuge der Zertifizierung nach IEC 61508 SIL3 geprüft.

Die Funktionen und Auslegungsvorgaben unter Sicherheitsaspekten resultieren aus der Qualifizierungsfähigkeit gemäß IEC 61508 SIL3. Geeignete analytische Maßnahmen zur Fehlervermeidung bei der Entwicklung konnten anhand der vorliegenden Hard- und Softwareprüfkonzepte nachvollzogen werden. Sowohl der Hardwareaufbau als auch der Softwareaufbau sind in der vorliegenden Dokumentation /19/, /20/ beschrieben und lassen konstruktive Maßnahmen zur Fehlervermeidung bei der Hard- und Softwareentwicklung erkennen. Die Programmlaufzeiten sind deterministisch und der Programmablauf ist streng zyklisch. Weiter sind in der Systemsoftware des CSC01 Diagnosemaßnahmen zur Fehlererkennung und -beherrschung im Programmablauf implementiert. Die implementierten Maßnahmen zur Fehlererkennung und -beherrschung in der Datenkommunikation basieren auf dem White-Channel-Prinzip.

Zusammenfassend kann festgestellt werden, dass der Typvertreter II CANopen Safety Chip die Forderungen der IEC 61508 SIL3 für eine sicherheitsgerichtete Kommunikation erfüllt. Obwohl das grundlegende Protokoll CAN einen ereignisorientierten Kommunikationsablauf realisiert, wird durch die zusätzlichen Eigenschaften der Sicherheitsvariante CANopen safety ein deterministischer Kommunikationsablauf sichergestellt. Die vorliegenden Unterlagen dokumentieren die Entwicklung und Qualitätssicherung ausführlich. Die Zertifizierung des Applikationsproduktes sowie die ordnungsgemäße Integration des CSC01 (z. B. Watchdog) in ein fertiges Herstellerprodukt müssen gesondert durchgeführt werden. Im Gegensatz zu Typvertreter I ist der CSC01 ein reines Businterface, das von einem Applikationshersteller in ein Endprodukt integriert werden muss. Die anhand des



Industrie Service

Fragenkatalogs zusammengestellten Informationen aus dem verfügbaren Unterlagenstand haben keine grundsätzlichen Anhaltspunkte gegen den Einsatz in kerntechnischen Leittechniksystemen, die Sicherheitsfunktionen der Kategorien A und B ausführen, ergeben. Für den Einsatz in kerntechnischen Anlagen wären aber noch ergänzende Unterlagen und Nachweise für das fertig integrierte Gerät bzw. System zu prüfen.

6 Zusammenfassung und Ausblick

In diesem Forschungsvorhaben wurde der Einsatz von digitaler Signalübertragung in Leittechnik mit sicherheitstechnischer Bedeutung (Kategorien A und B) in Kernkraftwerken untersucht. Die Ergebnisse dieser Arbeit legen wesentliche Aspekte für den Einsatz sicherheitsgerichteter Bussysteme in der Sicherheitsleittechnik von Kernkraftwerken und die im kerntechnischen Regelwerk relevanten Anforderungen dar.

Einleitend wurden die durch den Einsatz rechnergestützter Bussysteme verursachte Veränderung der Automatisierungsstrukturen und deren Auswirkungen dargestellt. Anschließend wurden relevante Anforderungen für digitale Signalübertragung aus dem kerntechnischen Regelwerk zusammengestellt. Hierbei wurden auf Ebene der Gesamtanlage relevante Anforderungen hinsichtlich Aufrechterhaltung des Defence-in-Depth-Konzeptes und der verfahrenstechnischen Redundanz und Diversität der Anlage identifiziert. Auf Leittechniksystemebene bestehen Anforderungen an die Systemarchitektur und die Unabhängigkeit von Teilsystemen. Bezüglich des Busprotokolls werden Anforderungen an Realisierung, Performance, Fehlererkennung und -beherrschung gestellt. Weiterhin bestehen Anforderungen an die Security sowie an die Kabel und Kabelverlegung.

Für die Realisierung von Sicherheitsbussystemen wurden die zwei unterschiedlichen Konzepte zur Beherrschung der spezifischen Fehlertypen (Grey-Channel und White-Channel) vorgestellt. Die prinzipielle Funktionsweise des Buszugriffsverfahrens von Standardbussystemen wurde erläutert und eine Marktrecherche der zurzeit am Markt erhältlichen Sicherheitsbussysteme durchgeführt.

Für eine nähere Betrachtung wurden zwei Typvertreter (PROFIsafe und CANopen Safety Chip) ausgewählt, die beide bereits nach IEC 61508 SIL3 zertifiziert wurden. Die Typvertreter wurden detailliert beschrieben, der Fragenkatalog des Forschungsvorhabens SR 2422 beantwortet und ausgewertet. Der Fragenkatalog wurde hierzu hinsichtlich der Spezifika von digitaler Signalübertragung entsprechend erweitert.



Die in den Fragekatalogen zusammengetragenen Informationen haben keine grundsätzlichen Anhaltspunkte ergeben, die prinzipiell gegen einen Einsatz von digitaler Signalübertragung in Leittechniksystemen in Kernkraftwerken, die Sicherheitsfunktionen der Kategorien A und B ausführen, sprechen. Allgemein gültige Vor- oder Nachteile der unterschiedlichen Realisierungskonzepte für Sicherheitsbussysteme konnten anhand der betrachteten Typvertreter nicht festgestellt werden.

Für konkrete Einsatzfälle sind jedoch die im Anhang III zusammengestellten Anforderungen zu berücksichtigen. Insbesondere sind die Systemarchitektur und die damit in Zusammenhang stehende Bustopologie zu bewerten, da diese einen Schwerpunkt der Anforderungen darstellen. Die damit in Zusammenhang stehenden Aspekte sollten in einer eigenen umfassenden Betrachtung behandelt werden. Ein weiterer wichtiger Aspekt für die einsatzspezifische Auslegung und Bewertung von digitalen Interfacebaugruppen stellt das implementierte Verhalten als Reaktion auf erkannte Fehler dar. Hierzu ist einsatzspezifisch zu überprüfen, inwieweit aus diesem Fehlerverhalten, insbesondere unter der Berücksichtigung von Fehlerkombinationen, ein Fail-Safe-Verhalten auf Systemebene erreicht werden kann.

7 Abkürzungsverzeichnis

ASIC	Application Specific Integrated Circuit
BIA	Berufsgenossenschaftliches Institut für Arbeitssicherheit
CAN	Controller Area Network
CiA	CAN in Automation
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check (Datensicherungsmethode)
CSMA	Carrier Sense Multiple Access
CSMA/CA	Collision Avoidance
CSMA/CD	Collision Detection
DIN	Deutsches Institut für Normung
EMV	Elektromagnetische Verträglichkeit
EPSC	Ethernet Powerlink Standardization Group
IEC	International Electrotechnical Commission
ISO	International Standard Organisation
KID	Konfigurations-Identifikations-Dokument
LAN	Local Area Network
LWL	Lichtwellenleiter
ODVA	Open DeviceNET Vendors Association



Industrie Service

OSI	Open System Interconnection
PNO	PROFIBUS Nutzerorganisation
SIL	Safety Integrity Level
SPS	Speicherprogrammierbare Steuerung



8 Normenverzeichnis

- /N1/ BMU/BMI
Sicherheitskriterien für Kernkraftwerke
Stand 09/83
- /N2/ RSK
Leitlinien für Druckwasserreaktoren
Stand: 01/97
- /N3/ KTA 3501
Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems
Stand: 06/85
- /N4/ KTA 3904
Warte, Notsteuerstelle und örtliche Leitstände in Kernkraftwerken
Stand: 08/88
- /N5/ IAEA NS-R-1
Safety Requirements: Safety of Nuclear Power Plants: Design
Stand: 09/00
- /N6/ IAEA NS-G-1.1
Safety Guide: Software for Computer Based Systems Important to Safety in Nuclear Power Plants
Stand: 09/00
- /N7/ IAEA NS-G-1.3
Safety Guide: Instrumentation and Control Systems Important to Safety in Nuclear Power Plants
Stand: 03/02



- /N8/ IEC 60709
Nuclear Power Plants
Separation of I&C Systems Important to Security
Stand 01/03
- /N9/ IEC 60987
Programmed Digital Computers Important to Safety for Nuclear Power Stations
Stand: 11/89
- /N10/ IEC 61226
Nuclear Power Plants
Instrumentation and Control Systems Important for Safety
Classification
Stand: 02/05
- /N11/ IEC 61508
Functional safety of electrical/electronic/programmable electronic safety-related systems
- Part 1 General requirements
Stand 12/98
- Part 2 Requirements for electrical/electronic/programmable electronic safety-related systems
Stand: 05/00
- Part 3 Software requirements
Stand: 12/98
- Part 4 Definitions and abbreviations
Stand: 11/98

- Part 5 Examples of methods for the determination of safety integrity levels
Stand: 11/98
- Part 6 Guidelines on the application of IEC 61508-2 and IEC 61508-3
Stand: 04/00
- Part 7 Overview of measures and techniques
Stand: 03/00
- /N12/ IEC 61513
Nuclear Power Plants
Instrumentation and Control Systems Important for Safety
General Requirements for Systems
Stand: 03/01
- /N13/ VDI/VDE 3527
Kriterien zur Gewährleistung der Unabhängigkeit von Sicherheitsfunktionen bei
der Leittechnik-Auslegung
Stand: 07/02
- /N14/ DIN V VDE 0801
Grundsätze für Rechner in Systemen mit Sicherheitsfragen
Stand: 01/90
- /N15/ EN 954-1
Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1:
Allgemeine Gestaltungsleitsätze
Stand: 1997
- /N16/ DIN V 19250
Fundamental aspects to be considered for measurement and control equipment
Stand: 05/94



- /N17/ 93/68/EEC
Low Voltage Directive
Directive on the harmonisation of the laws of Member States relating to electrical equipment designed for use within certain voltage limits
Stand: 02/73
- /N18/ prEN 50159-1
Railway Applications; Safety-Related Communication In Closed Transmission Systems
Stand: 1996
- /N19/ VDI/VDE 2180, part 3
Safeguarding of industrial processing plants by means of instrumentation and control technology
Stand: 1996
- /N20/ DIN VDE 0116, Chapter 8.7
Electrical equipment of furnaces
Stand: 10/89
- /N21/ EN 298, Chapters 9, 10
Automatic gas burner control systems for gas burners and gas burning appliances with or without fans
Stand: 10/93
- /N22/ EN 61131-2
Programmable controllers – equipment requirements and tests
Stand: 1995
- /N23/ EN 60204-1
Safety of machinery – Electrical equipment of machines
Stand: 1997

9 Literaturverzeichnis

Zertifikate und Prüfberichte

- /1/ TÜV Product Service GmbH TÜV SÜD Group, *Report on the Certificate Z2 01 12 20411 008 "Safety-related Software PROFIsafe Driver"*, München, Deutschland, 2004
- /2/ TÜV Automotive GmbH TÜV SÜD Group, *Report on the Certificate Z2 02 03 20411 009 "Safety-Related Programmable Systems SIMATIC S7 Distributed Safety"*, München, Deutschland, 2004
- /3/ TÜV Automotive GmbH TÜV SÜD Group, *Annex 1 of the Report on the Certificate "Safety-Related Programmable Systems SIMATIC S7 Distributed Safety"*, München, Deutschland, 2004
- /4/ TÜV Automotive GmbH TÜV SÜD Group, *Report on the Certificate Z2 03 04 38282 002 "Safety-Related Programmable Systems SIMATIC S7 F/FH Systems"*, München, Deutschland, 2004
- /5/ TÜV Automotive GmbH TÜV SÜD Group, *Annex 1 of the Report on the Certificate "Safety-Related Programmable Systems SIMATIC S7 F/FH Systems"*, München, Deutschland, 2005
- /6/ TÜV Industrie Service GmbH TÜV Rheinland Group, *Bericht über die Prüfung des CANopen Safety Chip CSC01*, Köln, Deutschland, 2004

Herstellerunterlagen

- /7/ PROFIBUS Nutzerorganisation e. V., *Draft Specification „PROFIsafe – Profile for Safety Technology on PROFIBUS DP and PROFINET IO“*, Karlsruhe, Deutschland, 2005

- /8/ Siemens AG, *Sicherheitstechnik in SIMATIC S7*, Systembeschreibung, Bereich Automation and Drives, Nürnberg, Deutschland, 2004
- /9/ Siemens AG, *Automatisierungssysteme S7 F/FH*, Handbuch, Bereich Automation and Drives, Nürnberg, Deutschland, 2004
- /10/ Siemens AG, *Automatisierungssystem S7-300 Fehlersichere Signalbaugruppen*, Handbuch, Bereich Automation and Drives, Nürnberg, Deutschland, 2004
- /11/ Siemens AG, *Dezentrales Peripheriegerät ET 200M*, Handbuch, Bereich Automation and Drives, Nürnberg, Deutschland, 2002
- /12/ CAN in Automation, *CANopen – Framework for safety-relevant communication*, Erlangen, Deutschland, 2005
- /13/ SYSTEC electronic GmbH, *Produktanforderungen – CANopen Safety Chip CSC01*, Greiz, Deutschland, 2003
- /14/ SYSTEC electronic GmbH, *Sicherheitskonzept – CANopen Safety Chip CSC01*, Greiz, Deutschland, 2003
- /15/ SYSTEC electronic GmbH, *Verifikations- und Validierungsplan – CANopen Safety Chip CSC01*, Greiz, Deutschland, 2003
- /16/ SYSTEC electronic GmbH, *Hardwareprüftest und Hardwareprüfergebnisse – CANopen Safety Chip CSC01*, Greiz, Deutschland, 2003
- /17/ SYSTEC electronic GmbH, *Softwareprüftest und Softwareprüfergebnisse – CANopen Safety Chip CSC01*, Greiz, Deutschland, 2003
- /18/ SYSTEC electronic GmbH, *Technische Dokumentation und Nutzerhandbuch – CANopen Safety Chip CSC01*, Greiz, Deutschland, 2003

- /19/ SYSTEC electronic GmbH, *Hardwaredesign – CANopen Safety Chip CSC01*, Greiz, Deutschland, 2003
- /20/ SYSTEC electronic GmbH, *Software design – CANopen Safety Chip CSC01*, Greiz, Deutschland, 2003

Kataloge, Prospekte und Artikel

- /21/ PROFIBUS International, *PROFIBUS Technologie und Anwendungen – Systembeschreibung*, Support Center, Karlsruhe, Deutschland, 2002
- /22/ Dr. H.-T. Fritzsche, *Der Sicherheits-Bus – Anforderungen und ihre Umsetzung*, Elektronik, Ausgabe 16, Poing, Deutschland, 1999
- /23/ *Sichere Netzwerkkommunikation*, Sicherheit + Management, Ausgabe 4/05, Seiten 96-97, GIT Verlag, Darmstadt, Deutschland, 2005
- /24/ Elan Schaltelemente GmbH & Co. KG, *ESALAN-Systeme: Programmierbare elektronische System mit Sicherheitsfunktion – Produktübersicht*, Wettenberg, 2004
- /25/ Dr. Wratil, *Safety related Data Transfer for EPL*, Innotec GmbH, EPLG_S Working Group, 2004
- /26/ F. Handermann, *Communication with SafeEthernet*, PRAXIS Profiline – Industrial Ethernet, Ausgabe 4/02, Seite 2, 2002
- /27/ Dr. O. Madelung, *Sicherheitsgerichtete Kommunikation: AS-Interface goes Safety*, iee, 44. Jahrgang, Ausgabe 4, Seiten 118-120, 1999

Literatur

- /28/ D. Reinert, F. Adams, *Sichere Bussysteme für die Automation*, Verlag Hüthig, Heidelberg, Deutschland, 2001

- /29/ TÜV Anlagentechnik GmbH, TÜV Rheinland Group, *Anwendung von Bussystemen in der Anlagensicherheit der Chemie-Industrie*, Forschungsvorhaben 35/00, München, Deutschland, 2000
- /30/ R. D. Schraft, G. Brandenburg, K. Bender, *Tagungsband SPS/IPC/DRIVES 2004*, Seiten 51-59, Nürnberg, Deutschland, 2004
- /31/ TÜV Industrie Service GmbH TÜV SÜD Group, *Anforderungen an rechnergestützte periphere Komponenten des Sicherheitssystems in Kernkraftwerken*, Abschlussbericht zu dem Vorhaben SR 2422, München, 2003
- /32/ Hauptverband der gewerblichen Berufsgenossenschaften HVBG, *Grundsatz für die Prüfung und Zertifizierung von „Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten“*, Fachausschuss Elektrotechnik, Prüf- und Zertifizierungsstelle, Köln, Deutschland, 2002
- /33/ B. Adamski, *Safety Bus Design Requirements for Process Industry Sector Applications*, Invensis – Premier Consulting Services, Irvine, Kalifornien, USA
- /34/ IEC, *Functional Safety and IEC61508 – A basic guide*, Internet: <http://www.iec.ch/functionalsafety>, 2004
- /35/ SAMSON AG, *Kommunikationsnetze – Teil 1 Grundlagen*, Internet: <http://www.samson.de>, Frankfurt, 2004



Anhang I: Ausgefüllter Fragenkatalog Typvertreter I

Inhalt:

Fragenkatalog zum Typvertreter I (PROFI-safe) mit 28 Seiten

1 Projektplanung und Aufbau der Dokumentation

1.1.1 Welches Vorgehensmodell wurde der Entwicklung zugrunde gelegt (z. B. Verfahrens-Modell, V-Modell)?

Das in der IEC 61508 festgelegte V-Modell wurde der Entwicklung zugrunde gelegt.

1.1.2 Gibt es eine Liste sämtlicher, entsprechend den Phasen des Vorgehensmodells, geordneter Dokumente?

Die in den einzelnen Phasen zu erstellenden Unterlagen werden in einer allgemeinen Planungsunterlage von Siemens A&D für die Entwicklung von fehlersicheren Komponenten aufgelistet.

1.1.3 Sind die einzelnen Phasen des Lebenszyklus des Produktes und die zugehörigen Aktivitäten detailliert festgelegt?

Die Phasen und Aktivitäten sind in der allgemeinen Planungsunterlage von Siemens A&D für die Entwicklung von fehlersicheren Komponenten festgelegt.

1.1.4 Gibt es einen produktspezifischen Projektplan? Wenn ja, was wurde dort festgelegt?

Auf der Basis der allgemeinen Planungsunterlage von Siemens A&D für die Entwicklung von fehlersicheren Komponenten wurde auch für die Interface-Komponenten eine produktspezifische Planungsunterlage erstellt, in der die spezifischen Festlegungen zum Qualitätsmanagement festgelegt wurden.

1.1.5 Gibt es einen produktspezifischen Qualitätssicherungsplan (oder -konzept) oder ein vergleichbares Dokument?

Die produktspezifische Planungsunterlage umfasst auch einen produktspezifischen Qualitätssicherungsplan.

1.1.6 Gibt es Festlegungen zu den verantwortlichen Personen, Abteilungen und Organisationen für jede Phase des Lebenszyklusses?

Wurden insbesondere Verifikations- und Validierungsaufgaben von den Implementierungsaufgaben getrennt?

In der Planungsunterlage erfolgt die Festlegung der verantwortlichen Personen für die einzelnen Aktivitäten der Entwicklungsphasen.

Der Modultest wird hierbei immer von Personen, die nicht an der Entwicklung des jeweiligen Testobjekts beteiligt waren, durchgeführt. Für den Systemtest besteht eine von der Entwicklung getrennte Abteilung. Durch die Typprüfung des TÜV SÜD erfolgte eine herstellerunabhängige Prüfung.

1.1.7 Unterliegen die relevanten Dokumente hinsichtlich ihrer Überarbeitung, Prüfung und Freigabe einem angemessenen System der Dokumentenlenkung?

Aus den Standardangaben auf den Dokumentenblättern ist eine anforderungsgerechte Dokumentenlenkung gemäß DIN EN ISO 9001:2000 erkennbar.

1.2.1 Gibt es eine Anforderungsspezifikation (Lastenheft)?

Wenn ja, sind dort

**Funktionsanforderungen,
Sicherheitsanforderungen,
Normen die der Entwicklung bzw. Qualifizierung zugrunde gelegt
wurden**

enthalten?

Die Funktionen sind in einem Lastenheft beschrieben. Alle sicherheitstechnisch relevanten Anforderungen sind darüber hinaus in der Safety Requirement Specification gemäß IEC 61508 festgelegt.

1.2.2 Gibt es eine Systemspezifikation (Pflichtenheft, Entwurfsspezifikation) für Hardware und Software?

Hierzu wurden ein Systempflichtenheft und Produktpflichtenhefte erstellt.

1.2.3 Wie ist die Entwicklungsdokumentation aufgebaut?

Neben den Pflichtenheften wurden zur Spezifikation der Entwicklung Entwicklungsunterlagen erstellt.

**1.2.4 Gibt es eine Prüfspezifikation für die Komponente?
Wie ist die Prüfdokumentation aufgebaut?**

Es bestehen produktspezifische Testkonzepte und Testberichte

1.2.5 Können die kompletten Softwarequellen (Sourcecode) vorgelegt werden?

Der Source-Code des PROFIsafe Treibers lag bei der Typprüfung mit dem TÜV-Prüfbericht "Safety-related Software PROFIsafe Driver", Bericht-Nr.: 70013527 vom 09.07.2004 vor.

1.3.1 Gibt es detaillierte Festlegungen zum Konfigurations- und Änderungsmanagement für die Hard- und Software? Wenn ja, wo ist diese dokumentiert?

Hierzu besteht eine A&D eigene Anweisung.

1.3.2 Gibt es ein KID (Konfigurations-Identifikations-Dokument)?

Mit dem "Annex 1" zum Prüfbericht "SIMATIC S7 F/FH Systems" liegt ein Dokument vor, das die Softwarestände und die Hardwarestände der typgeprüften Versionen festhält.

1.4 Welche Normen wurden der Entwicklung zugrunde gelegt?

Im Rahmen der Typprüfung wurde die Einhaltung folgender Normen und Richtlinien geprüft:

- 93/68/EEC Low Voltage Directive (Directive on the harmonisation of the laws of Member States relating to electrical equipment designed for use within certain voltage limits)
- IEC 61508:1999, parts 1 to 7, SIL 1-3 (Functional Safety, Safety-related systems)
- DIN V 19250:1994 (Fundamental aspects to be considered for measurement and control equipment)
- DIN V VDE 0801:1990 with Amendment A1:1994, AK 1-6 (Principals for computers in safety-related systems)
- prEN 50159-1:1996 (Railway Applications; Safety-Related Communication In Closed Transmission Systems)
- VDI/VDE 2180:1996, part 3 (Safeguarding of industrial processing plants by means of instrumentation and control technology)
- DIN VDE 0116:1989, Chapter 8.7 (Elektrical equipment of furnaces)
- EN 298:1993, Chapters 9,10 (Automatic gas burner control systems for gas burners and gas burning appliances with or without fans)
- EN 954-1:1997 Safety Categories 2-4 (Safety of machinery; Safety-related parts of control systems, Part 1 "General principles for design")
- EN 61131-2:1995 (Programmable controllers - equipment requirements and tests)
- EN 60204-1:1997 (Safety of machinery - Electrical equipment of machines)

2 Funktionen und Auslegungsvorgaben unter Sicherheitsaspekten

2.1 Gibt es eine detaillierte Beschreibung der Leittechnik-, Überwachungs- und Unterstützungsfunktionen, die für nicht an der Entwicklung beteiligte Personen nachvollziehbar ist?

Die Beschreibung ist in der Systembeschreibung "Sicherheitstechnik in SIMATIC S7" und der Software-Spezifikation "PROFIsafe - Profile for Safety Technology on PROFIBUS DP and PROFINET IO" für den PROFIsafe-Treiber enthalten. Die Beschreibung wurde im Rahmen der Typprüfung nach IEC 61508 überprüft.

2.2 Gibt es eine detaillierte Beschreibung der Aufgaben und Funktionen, die die Software zu erfüllen hat, die für nicht an der Entwicklung beteiligte Personen nachvollziehbar ist?

Die Beschreibung ist in der Software-Spezifikation "PROFIsafe - Profile for Safety Technology on PROFIBUS DP and PROFINET IO" für den PROFIsafe-Treiber enthalten. Die Beschreibung wurde im Rahmen der Typprüfung nach IEC 61508 überprüft.

2.3 Gibt es eine detaillierte Beschreibung der Konfigurations- und Parametriermöglichkeiten?

Die Benutzerdokumentation "Automatisierungssysteme S7 F/FH" und "Automatisierungssystem S7-300 Fehlersichere Signalbaugruppen" wurde vom TÜV SÜD im Zusammenhang mit der Zertifizierung inspiziert. Sie enthält die für die sicherheitstechnische Verwendung des S7 F/FH Systems durch einen Anwender/Entwickler notwendigen Informationen.

2.4 Gibt es mehrere Varianten der Komponente (z. B. eine Sondervariante für den sicherheitstechnischen Einsatz)? Wenn ja, wie unterscheiden sich diese hinsichtlich Hard- und Software voneinander?

Die Software PROFIsafe Treiber mit der Kommunikationsfunktion wird auf allen Zentralbaugruppen und fehlersicheren Peripheriebaugruppen der Gerätefamilie integriert. Die fehlersicheren Signalbaugruppen, die den PROFIsafe Treiber enthalten, unterscheiden sich im Wesentlichen dadurch von den Standardbaugruppen des S7-300-Baugruppenspektrums, dass sie intern zweikanalig (2 Prozessoren) aufgebaut sind.

2.5 Gab es eine Entwicklungsvorgabe, dass Betriebs- und sicherheitstechnisch wichtige Funktionen unabhängig voneinander arbeiten müssen?

In die fehlersicheren Peripheriekomponenten wurden keine betrieblichen Funktionen implementiert.

2.6 Gab es Entwicklungsvorgaben hinsichtlich besonderer (Selbst-) Überwachungsfunktionen? Wenn ja, gibt es eine detaillierte Beschreibung dieser Funktionen?

Aufgrund des der Entwicklung zugrunde liegenden Herstellerziels der Qualifizierungsfähigkeit gemäß IEC 61508 SIL3 ist von entsprechenden Entwicklungsvorgaben auszugehen.

Eine Zusammenstellung der (Selbst-)Überwachungsfunktionen befindet sich in den Tabellen 9.9 und 9.10 im Dokument "Automatisierungssystem S7-300 Fehlersichere Signalbaugruppen".

2.7 Gab es Entwicklungsvorgaben hinsichtlich fehlerbeherrschender Strukturen und Maßnahmen (z. B. Fail-Safe-Verhalten, fehlertoleranter Aufbau, Verhinderung unzulässiger Operationen)?

Aufgrund dem der Entwicklung zugrunde liegenden Ziel der Qualifizierungsfähigkeit gemäß IEC 61508 SIL3 ist von entsprechenden Entwicklungsvorgaben auszugehen.

Die Peripheriebaugruppen zur Digitalein-/ausgabe sind intern redundant aufgebaut.

Das fehlersichere PROFIsafe Protokoll besitzt eine Hamming-Distanz von 4. Das bedeutet, dass durch Prüfsummen bis zu 3 Bitfehler korrigiert werden können. Ab 4 Bitfehlern kann der Fehler noch detektiert, nicht aber korrigiert werden.

Grundlage des Sicherheitskonzeptes ist es, dass bei erkannten Fehlern, die die Funktion beeinflussen können, ein definierter Fehlerzustand, der sogenannte "sichere Zustand" in der IEC 61508 Terminologie eingenommen wird.

Hinweis: Der Einsatz von gemäß IEC 61508 zertifizierten Geräten in der Industrie erfolgt grundsätzlich für sicherheitsgerichtete Funktionen, die einen eindeutigen Fail-Safe-Zustand (z. B. Maschinenabschaltung, Stromabschaltung, etc.) aufweisen.

2.8 Gab es Entwicklungsvorgaben zur Auslegung gegen besondere Umwelteinflüsse (EMV, induzierte Erschütterungen aus Erdbeben, KMV etc.)?

Aufgrund dem der Entwicklung zugrunde liegenden Ziel der Qualifizierungsfähigkeit gemäß IEC 61508 SIL3 ist von entsprechenden Entwicklungsvorgaben auszugehen.

Es fanden Prüfungen zu EMV, mechanischen und klimatischen Umgebungsbedingungen, Isolationsprüfungen und explosionsgefährdeten Bereichen Zone 2 statt.

2.9 Gab es Entwicklungsvorgaben hinsichtlich des Schutzes der gespeicherten Programme und Parameter gegen Veränderung?

Aufgrund dem der Entwicklung zugrunde liegenden Ziel der Qualifizierungsfähigkeit gemäß IEC 61508 SIL3 ist von entsprechenden Entwicklungsvorgaben auszugehen.

Ein Passwort schützt die F-Systeme vor unbefugtem Zugriff, d. h. gegen unerwünschtes Laden von Programmänderungen in die F-CPU vom Engineering System (ES) oder vom Programmiergerät (PG) aus.

2.10 Gab es Entwicklungsvorgaben zu den Prinzipien zur Sicherstellung eines möglichst deterministischen Verhaltens (z. B. einer streng zyklischen Abarbeitung des Hauptprogrammes)?

Aufgrund dem der Entwicklung zugrunde liegenden Ziel der Qualifizierungsfähigkeit gemäß IEC 61508 SIL3 ist von entsprechenden Entwicklungsvorgaben auszugehen.

Das zugrunde liegende PROFIBUS DP Protokoll ist ein Master-Slave Polling-Verfahren, welches seinem Konzept nach streng zyklisch arbeitet.

2.11 Gab es Entwicklungsvorgaben hinsichtlich des Ausfall- bzw. Fehlerverhaltens der Komponente?

Aufgrund dem der Entwicklung zugrunde liegenden Ziel der Qualifizierungsfähigkeit gemäß IEC 61508 SIL3 ist von entsprechenden Entwicklungsvorgaben auszugehen.

Grundlage des Sicherheitskonzeptes ist es, dass bei allen erkannten Fehlern, die die Funktion beeinflussen können, der sichere Zustand gemäß IEC 61508 eingenommen wird. Bei digitaler F-Peripherie ist das z. B. der Wert "0".

Die beiden in einer fehlersicheren Signalbaugruppe integrierten Prozessoren überwachen sich gegenseitig und testen automatisch die Ein- bzw. Ausgabeschaltungen. Die F-CPU kommuniziert mit der fehlersicheren Signalbaugruppe über das sicherheitsgerichtete Busprofil PROFIsafe. Peripherie- oder Kommunikationsfehler führen zur Passivierung der betroffenen Kanäle oder F-Peripherie aber nicht zum STOPP der F-CPU. Nach der Fehlerbehebung muss eine Wiedereingliederung (Depassivierung) der F-Peripherie erfolgen.

2.12 Gab es Entwicklungsvorgaben, dass die Komponente (z. B. steckbare Baugruppe) bei Betrieb austauschbar ist?

Die fehlersicheren Signalbaugruppen (F-SMs) können wie alle Standard-Signalbaugruppen in S7-300 bzw. ET 200M gesteckt und gezogen werden. Ein Baugruppentausch im Sicherheitsbetrieb wird als Fehler bei der sicherheitsgerichteten Kommunikation (Kommunikationsfehler) zwischen der F-CPU und der ausgetauschten F-SM gemeldet.

2.13 Gab es Entwicklungsvorgaben hinsichtlich einer energetischen, datentechnischen und funktionalen Entkopplung an den Schnittstellen zur Kraftwerksanlage (Fehlerfortpflanzungssperren)?

Aufgrund dem der Entwicklung zugrunde liegenden Ziel der Qualifizierungsfähigkeit gemäß IEC 61508 SIL3 ist von entsprechenden Entwicklungsvorgaben auszugehen.

Es erfolgt eine Potentialtrennung auf den Ein-/Ausgabemodulen zwischen den Kanalgruppen der Ein-/Ausgänge sowie der Kanäle zum Rückwandbus und zur Spannungsversorgung der Elektronik. Der Produktkatalog "Industrielle Kommunikation für Automation and Drives", Katalog IK PI 2005 der Siemens AG führt für die Entkopplung der PROFIBUS-Schnittstelle eine Isolationsspannung von 500 V auf.

Eine datentechnische Entkopplung erfolgt durch den festen Zyklus der Kommunikation ohne gegenseitige zeitliche Abhängigkeit zwischen Sender und Empfänger.

2.14 Gab es Entwicklungsvorgaben zur Sicherstellung von konstanten Betriebsbedingungen der Komponente (wie statische Zuordnung von Systemressourcen, so dass die Systemfunktionen unabhängig vom Prozess gleichbleibend beansprucht werden, zyklische Bearbeitung der Anwenderfunktionen, Verzicht auf prozessabhängige Interrupts, vorbeugende Maßnahmen gegen Software-Exceptions)?

Aufgrund dem der Entwicklung zugrunde liegenden Ziel der Qualifizierungsfähigkeit gemäß IEC 61508 SIL3 ist von entsprechenden Entwicklungsvorgaben auszugehen.

Konstante Reaktionszeiten werden in der SIMATIC mit einem äquidistanten DP-Buszyklus, der Synchronisation des Anwenderprogramms auf den DP-Buszyklus und der taktsynchronen Übertragung der E/A-Daten auf die Peripheriebaugruppen realisiert. Die E/A-Daten werden in definierten und gleichbleibenden (taktsynchronen) Zeitabständen über den Rückwandbus des DP-Slave auf die Peripheriebaugruppen übertragen und taktsynchron ausgegeben. Die maximale Schwankung beträgt 10 µs.

2.15 Gab es Entwicklungsvorgaben zur Performance (Zeitverhalten, zu berücksichtigende Belastungen, Anlaufverhalten, Genauigkeit, maximale Auslastung des Prozessors, zu erwartende Belastungen)?

Aufgrund dem der Entwicklung zugrunde liegenden Ziel der Qualifizierungsfähigkeit gemäß IEC 61508 SIL3 ist von entsprechenden Entwicklungsvorgaben auszugehen.

Die Reaktionszeiten der fehlersicheren Signalbaugruppen gehen in die Berechnung der Reaktionszeit des SIMATIC Safety Integrated Systems ein. Für fehlersichere Digitaleingänge gibt die Reaktionszeit die Zeit zwischen einem Signalwechsel am Digitaleingang bis zum sicheren Bereitstellen des Sicherheitstelegramms am Rückwandbus an. Für fehlersichere Digitalausgänge gibt die Reaktionszeit die Zeit zwischen einem ankommenden Sicherheitstelegramm vom Rückwandbus bis zum Signalwechsel am Digitalausgang an. Bei Vorhandensein eines Fehlers in den Ein-/Ausgabemodulen verlängert sich die Reaktionszeit um die parametrierbare Diskrepanzzeit.

Aufgrund der damit bekannten Reaktionszeit der einzelnen Komponenten lässt sich das Zeitverhalten des Systems exakt angeben.

2.16 Wurden verschiedene Betriebsarten definiert? Wenn ja, wo sind diese dokumentiert?

In den vorliegenden Unterlagen werden keine unterschiedlichen Betriebsarten beschrieben.

2.17 Wurde eine Gefährdungs- / Risikoanalyse für die Komponente durchgeführt?

Es wurde eine Gefährdungs-/Risikoanalyse im Rahmen der IEC 61508 Zertifizierung durchgeführt.

2.18 Wurden Maßnahmen getroffen, um die Lieferbarkeit der verwendeten Hardwarekomponenten dauerhaft sicherzustellen? Wenn ja, wie sehen diese aus?

Zum Einsatz kommen Bauteile mit einem weit gestreuten Einsatz im Automotiv/Industrie-Einsatz. Eine spezielle Stelle bei A&D verwaltet die Vorzugslieferanten sowie Second-Source-Lieferanten und sorgt für Einlagerung von Bauteilen bei Abkündigungen.

2.19 Wurden über die Spezifikationen hinausgehende verborgene Funktionalitäten implementiert, die im Entwicklungsprozess als erforderlich angesehen wurden (z. B. zu Entwicklungszwecken, zur Wartung und Diagnose)?

Es wurde ein Trace-Tool implementiert, das für Diagnosen des Herstellers vorgesehen ist. Dieses SW-Tool läuft ständig im Hintergrund, kann aber nur durch Anwendung eines speziellen HW-Adapters benutzt werden.

2.20 Wie werden die systemimmanenten Eigenschaften der derzeit eingesetzten nicht digital ausgeführten Komponente bei der rechnergestützten Komponente abgebildet?

Derzeit werden festverdrahtete Verbindungen eingesetzt. Diese zeichnen sich durch verzögerungsfreie Übertragung und Parallelität aus. Bei der Verwendung eines Bussystems muss die von der Zykluszeit abhängige Verzögerung berücksichtigt werden. Aufgrund der deterministischen Funktionsweise des zugrunde liegenden Bussystems PROFIBUS DP ist es möglich, die maximale Verzögerungszeit anzugeben. Diese muss bei der Systemauslegung berücksichtigt werden. Parallele Datenübertragung ist für mehrere Signale innerhalb eines Datenpaketes grundsätzlich möglich.

Der Einfluss von Einzelfehlern wirkt sich bei festverdrahteten Verbindungen jeweils nur auf ein Signal aus. Bei Bussystemen muss der gleichzeitige Ausfall einer Vielzahl von Signalen unterstellt werden.

Die Fehlerquellen Kurzschluss und Drahtbruch müssen bei festverdrahteten Verbindungen detektiert werden. Aufgrund der zyklischen Nachrichtenübertragung und des zentralenbasierten Pollingverfahrens werden derartige Ausfälle des Bus-Kabels erkannt. Die neu hinzukommenden Fehlertypen (Datenverfälschung, Verlust, Verzögerung, falsche Reihenfolge, Wiederholung) werden durch die Selbstüberwachungsfunktionen ebenfalls erkannt.

3 Analytische Maßnahmen zur Fehlervermeidung bei der Entwicklung

3.1 Wurde ein Prüfkonzert für die Komponente zugrunde gelegt? Wenn ja, enthält dieses Aussagen zu folgenden Fragestellungen:

Wann wird geprüft (z. B. Festlegungen zu Reviews)?

Was für Prüfmittel kommen zum Einsatz?

Wer führt die Prüfungen durch (Trennung Entwicklung /Test)?

Wie wurden die Prüfungen dokumentiert (Protokolle)?

Angaben hierzu bestehen in der allgemeinen und der produktspezifischen Planungsunterlage sowie in dem produktspezifischen Testkonzept. Die Dokumentation von durchgeführten Prüfungen erfolgt in Testberichten.

3.2.1 Was für Typprüfungen wurden durchgeführt?

Wurden im Rahmen der Typprüfungen auch

- EMV-Prüfungen,
- Prüfungen der Auslegung gegen induzierte Erschütterung (Schwingen und Schocken),
- Prüfung zur Auslegung gegen besondere Umwelteinflüsse

durchgeführt?

Es wurde eine Typprüfung für das System Siemens Integrated Safety und den Software-Treiber PROFIsafe nach IEC 61508 durchgeführt. Außerdem wurden klimatische und mechanische Typprüfungen sowie Prüfungen zur elektromagnetischen Verträglichkeit durchgeführt (siehe Verzeichnis der geprüften Normen in 1.4).

3.2.2 Wurden statische und dynamische Tests der Software durchgeführt?

Gemäß dem Hersteller wurden sowohl statische Tests (Reviews, Erfüllung von MISRA) als auch dynamische Tests der Software durchgeführt. Die dynamischen Tests gliedern sich in Modultests in einer Testumgebung, Integrationstests mit minimaler HW-Konfiguration und Systemtests mit maximalem HW-Ausbau sowie den abschließenden Validationstests zum Nachweis der Anforderungen der Safety Requirement Specification.

3.2.3 Gibt es einen Softwaretestbericht mit Angaben zu den durchgeführten statischen und dynamischen Tests?

Die statischen Tests wurden in Reviewberichten, die dynamischen Tests in Testberichten dokumentiert.

3.2.4 Welche Hard- und Software-Integrationstests wurden durchgeführt?

Als Integrationstest wurden Funktionstests in einer Minimalkonfiguration der HW durchgeführt.

**3.2.5 Welche Systemtests bzw. Systemintegrationstests wurden durchgeführt?
Wie wurden diese dokumentiert?**

Es wurde ein Systemtest mit maximal möglichem HW-Ausbau durchgeführt und ein Validationstest zum Nachweis der Anforderungen der Safety Requirement Specification. Die Tests sind im Testkonzept und in Testberichten dokumentiert.

3.3.1 Wurden die Ablaufreihenfolge, die Aufruf- und Anlaufbedingungen der Tasks überprüft?

Diese Prüfungen erfolgten im Systemtest.

3.3.2 Wurden spezielle Werkzeuge oder automatische Testhilfen für die Prüfung der Software eingesetzt? Wenn ja, welche?

Mit dem Entwicklungswerkzeug Rhapsody, in dem auch die Spezifikation der Software erfolgt, erfolgen auch eine automatische Testgenerierung und Testdurchführung.

3.3.3 Wurden Tests der Software in einer Emulationsumgebung durchgeführt (z. B. Softwareemulation, In-Circuit-Emulation (ICE))?

Wurde der Programmcode so instrumentiert, dass während der Testphasen Tracing-Informationen gewonnen werden können?

Im Rahmen des Modultests und des Integrationstests wurde ein ICE eingesetzt. Eine Programminstrumentierung war damit nicht nötig.

3.3.4 Wurden Simulations-Tools zur Prüfung der Software oder im Rahmen der Systemtests eingesetzt?

Es wurde ein von A&D entwickelter und zertifizierter ProfiSafe Layer-Tester, der für die Konformitätsprüfung von Produkten eingesetzt wird, verwendet.

3.3.5 Wurde eine Timing-Analyse durchgeführt?

Dies war ein Schwerpunkt beim Integrations- und Systemtest.

3.3.6 Erfolgte eine Überprüfung der Datenraten, Reaktionszeiten und des Verhaltens in Grenzsituationen (Performanceprüfungen)?

Diese Prüfungen erfolgten im Integrations- und Systemtest.

**3.3.7 Welche Validierungsprüfungen wurden durchgeführt?
Wurden insbesondere Maßnahmen zur Validierung von automatisch durch Werkzeuge erzeugte Software getroffen?**

Die Validationstests wurden zum Nachweis der Anforderungen aus der Safety Requirement Specification durchgeführt. Die auf der Basis der Spezifikation in Rhapsody automatisch erzeugte Software wurde im Rahmen der dynamischen Tests geprüft.

3.3.8 Wurden Prüfungen der (Mikrokontroller-)Hardware vor der HW/SW-Integration durchgeführt?

Nein

3.3.9 Erfolgte eine Überprüfung der Auslastung des Speichers und des Stacks?

Dies erfolgte im Rahmen des Integrationstests.

3.4 Wurde ein Verfahren festgelegt, wie mit festgestellten Fehlern umgegangen wird (z. B. Einteilung in Fehlerklassen)? Wenn ja, wo ist dieses dokumentiert?

Hierzu ist ein Verfahren in einer A&D-Verfahrensanweisung festgelegt. Es wird werkzeugunterstützt durchgeführt (ClearQuest).

3.5.1 Wurden spezielle methodische Verfahren zur Analyse möglicher Störungen, Fehler oder Ausfälle für die Komponente ggf. auf der Bauteil-/ Einzelkomponentenebene durchgeführt (z. B. FTA, FMEA)?

Eine Fehlerbetrachtung erfolgte im Rahmen der Zertifizierung gemäß IEC 61508.

3.5.2 Gab es Untersuchungen der Hard- und Software hinsichtlich des CCF (Common-Cause-Failure)-Potentials?

Spezifisch für Interfaces sind hierbei Fehler auf dem Bus sowie die Fehlerfortpflanzung von der Sender- auf die Empfangsseite zu betrachten. Gemäß Anhang B der IEC 61508-2 werden für zertifizierte Geräte bezüglich der systematischen Ausfälle fehlervermeidende Maßnahmen und Maßnahmen zur Beherrschung von Ausfällen getroffen. Dies bildet sich auch in den entsprechenden Kapiteln des vorliegenden Fragenkataloges ab (Kapitel 3, 5 und 6 bzw. Kapitel 7).

Zur quantitativen Ermittlung wurde ein heuristisches Verfahren im Rahmen der FMEA zur Ermittlung des Anteils von systematischen Fehlern (Beta-Faktor) angewandt.

4 Betrieb und Wartung, wiederkehrende Prüfungen

4.1 Gibt es einen Prüfmodus für Inbetriebsetzung und wiederkehrende Prüfungen (WKP)?

Nicht relevant für Interface-Baugruppen.

4.2 Welche Dokumentationsunterlagen gibt es für den Benutzer und den Service?

Gibt es

- ein Benutzerhandbuch?
- eine Bedienungsanleitung?
- eine Reparaturanleitung?
- eine Konfigurationsanleitung?
- Prüfanweisungen?

Folgende Dokumentationsunterlagen existieren:

- Sicherheitstechnik in SIMATIC S7 Systembeschreibung
- Automatisierungssystem S7-300 Fehlersichere Signalbaugruppen, Handbuch

4.3 Welche Festlegungen für den Benutzer gibt es, wenn während des Betriebes Abweichungen (Fehlermeldungen) auftreten?

Nicht relevant für Interface-Baugruppen.

4.4.1 Sind eine größere Anzahl identischer Komponenten unter vergleichbaren Einsatzbedingungen bereits über einen längeren Zeitraum eingesetzt?

Die Siemens S7 Produktreihe ist bereits langjährig unter vergleichbaren Bedingungen im industriellen Einsatz und ist betriebsbewährt.

4.4.2 Wurden besondere Möglichkeiten zur Gewinnung von Betriebsdaten oder Diagnosedaten vorgesehen?

Erkannte Fehler werden in den Diagnosepuffer der Ein-/Ausgabemodule F-SM und den Diagnosepuffer der CPU eingetragen und dem Sicherheitsprogramm in der F-CPU mitgeteilt.

4.4.3 Wurden die bisherigen Betriebserfahrungen mit der Komponente systematisch erfasst und nachvollziehbar und vertrauenswürdig dokumentiert?

Es erfolgt eine Erfassung von Rückläufern und Betriebserfahrungen in einer Datenbank.

4.4.4 Sind Ausfälle der Komponente bekannt? Wenn ja, wurden die Ursachen für Ausfälle der Komponente eingehend untersucht und dokumentiert?

Die Rückläufer- und Erfahrungs-Datenbank wird hinsichtlich Anhaltspunkten für erforderliche Änderungen untersucht.

4.4.5 Werden die sicherheitstechnisch wichtigen Funktionen der Komponente regelmäßig innerhalb eines kurzen Zeitintervalls angefordert?

Durch die Verwendung als Businterface mit zyklischer Datenübertragung ist eine ständige Anforderung gegeben.

5 Konstruktive Maßnahmen zur Fehlervermeidung bei der Hardwareentwicklung

5.1 Gibt es eine detaillierte Beschreibung der Hardware mit Angaben zur Struktur, Modularisierung etc., die für nicht an der Entwicklung beteiligte Personen nachvollziehbar ist?

Diese Beschreibung ist in den Pflichtenheften enthalten.

5.2 Welcher Mikrokontroller bzw. Mikroprozessor (Hersteller, Typ) wurde ausgewählt und was waren die Kriterien für die Auswahl?

Es wird seit einigen Jahren bei der S7-Entwicklung ein 32bit-Mikrocontroller von NEC eingesetzt. Auswahlkriterien waren die Verbreitung in der Elektronik/Automations-Welt und Performanceanforderungen.

5.3 Wie ist die Speicherorganisation der Komponente (von Neumann, (mod.) Harvard-Struktur) und wie erfolgt die Trennung von Daten und Programmen?

Programme sind im Flash-Speicher gespeichert, Daten im RAM.

5.4 Welche Programm- und Datenspeicher (Typ, Größe ...) sind eingesetzt? Wo ist dies dokumentiert?

Der Flash-Speicher für das Programm hat 126 kB. Zusätzlich ist ein RAM-Speicher für Daten vorhanden.

5.5 Erfolgt eine statische oder eine dynamische Speicherzuordnung für Daten und Programme? Wo ist dies dokumentiert?

Der Programmspeicher ist statisch zugeordnet.

5.6 Sind weitere "intelligente" Bausteine wie Buskontroller, LAN-Schnittstellen, ASIC, PLD etc. eingesetzt? Wenn ja, gibt es eine detaillierte Beschreibung dieser Bausteine und ihrer Funktionen?

Es sind noch ASICs und EPLDs eingesetzt. Die Funktionen sind in den Entwicklungsunterlagen beschrieben.

5.7 Wurde in der Hardware eine Trennung für sicherheitstechnisch wichtige und betriebliche Funktionen vorgesehen bzw. realisiert?

Bei Betrieb der Ein-/Ausgabemodule F-SM als fehlersichere Komponenten übernehmen diese ausschließlich sicherheitstechnische Aufgaben. Es besteht die Möglichkeit, die fehlersicheren Ein-/Ausgabemodule F-SM alternativ für betriebliche Funktionen zu verwenden. Ein Mischbetrieb fehlersicherer und betrieblicher Ein-/Ausgabemodule in einem SIMATIC Distributed Safety System ist möglich. Ein SIMATIC F/FH System lässt dies nicht zu.

5.8 Gibt es sicherheitstechnisch wichtige Funktionen, die in vom Mikrokontroller/Mikroprozessor unabhängiger Hardware realisiert wurden?

Nein

5.9 Erfolgte die Auslegung der Komponente mit Uhrzeit oder Kalender? Wenn ja, was wurde festgelegt um Probleme wie Sommer-/Winterzeit-Umschaltung und kritische Kalenderdaten (z. B. Schaltjahreffekte) zu lösen? Wo ist dies dokumentiert?

Die Verwendung von Uhrzeit- bzw. Kalenderfunktionen ist nicht dokumentiert.

5.10 Wurde die Hardware hinsichtlich zu erwartender Alterungseffekte analysiert und welche Reserven wurden hierfür berücksichtigt?

Die ELKOs für die Bereitstellung der Restenergie für notwendige Aufräumarbeiten nach einem Netzausfall wurden mit einer hohen Reserve ausgelegt, damit auch nach längeren Betriebszeiten ausreichende Energiereserven bereitstehen.

6 Konstruktive Maßnahmen zur Fehlervermeidung bei der Softwareentwicklung

6.1.1 Wie ist die Software der Komponente aufgebaut?

Die Software ist modulatorientiert aufgebaut.

6.1.2 Wurden spezielle Tools zur Versionsverwaltung eingesetzt? Wenn ja, welche?

Es wurde ClearCase von Rational Software eingesetzt.

6.1.3 Ist der Sourcecode gut strukturiert, lesbar und dokumentiert?

Der Source-Code lag nicht vor.

6.1.4 Wurden bei der Erstellung der Software spezielle Programmierrichtlinien berücksichtigt? Wenn ja, welche Festlegungen finden sich dort und wo sind diese dokumentiert?

Es wurden für die Erstellung der C- und Assembler-Source Coding-Standards zugrunde gelegt. Weiterhin wird eine statische Analyse gemäß MISRA durchgeführt.

6.2.1 Wie ist der Prozess zur Erzeugung des Maschinencodes gestaltet? Kamen Werkzeuge (Tools) für die automatische Generierung von Sourcecode zum Einsatz? Wenn ja, welche, und wo sind diese detailliert beschrieben?

Es wurde die Entwicklungsumgebung Rhapsody benutzt, die die grafische Programmierung erlaubt und daraus C erzeugt. Der C-Code wurde anschließend mit einem C-Compiler übersetzt.

6.2.2 Welche Programmiersprachen wurden verwendet?

Es wurde hauptsächlich in C und für einige Ausnahmen in Assembler programmiert.

6.2.3 Ist der Compiler (Übersetzer) durchgehend getestet und bewährt? Sind evtl. Einschränkungen bekannt? Wurden Compiler-Funktionen zur Optimierung des Codes benutzt? Werden neben den Standard-Bibliotheken noch weitere Bibliotheken benutzt?

Der verwendete Compiler ist bei Siemens A&D bewährt. Es werden keine Codeoptimierung und keine Bibliotheken benutzt.

6.2.4 Ist dynamisches Binden zugelassen?

Nein

- 6.3.1 Wie erfolgte die Modularisierung der Software und wie sind die systeminternen Schnittstellen definiert?
Welche Softwaremodule bzw. Komponenten gibt es?
Wie ist die Softwarestruktur aufgebaut?
Gibt es eine detaillierte Beschreibung der Softwarestruktur?
Gibt es eine detaillierte Beschreibung der Module
(Funktionsbeschreibung, Ein-/Ausgabewerte, etc)?**

Die Modularisierung erfolgte entsprechend der Entwurfsspezifikation. Sowohl die Softwarestruktur als auch die einzelnen Module sind in den Entwicklungsunterlagen detailliert beschrieben.

- 6.3.2 Erfolgte eine Modularisierung der Software in überschaubare Einheiten?**

Der Hersteller bestätigte dies.

- 6.3.3 Wurden Maßnahmen zur eindeutigen Identifikation von Softwareeinheiten getroffen? Wenn ja, wo sind diese dokumentiert?**

Der TÜV-Prüfbericht "Safety-related Software PROFIsafe Treiber" listet die CRC-Prüfsummen der zertifizierten Quellcode-Dateien auf.

- 6.3.4 Gibt es eine eindeutige Zuordnung von Modulen zu den in der Anforderungsspezifikation definierten Funktionen?**

Es gibt eine eindeutige Zuordnung von Modulen zu den in der Safety Requirement Specification enthaltenen Anforderungen.

- 6.4 Welche Taskstruktur und Übergangsbedingungen für die Taskwechsel gibt es?**

**Gibt es eine Taskbeschreibung?
Wie erfolgt die Synchronisation, Zuteilung des Prozessors?
Wo ist dies dokumentiert?**

Das Programm mit den Sicherheitsfunktionen wird zeitgesteuert über Interrupt zyklisch aufgerufen.

- 6.5 Wie sind bei mehreren Betriebsarten die Übergangsbedingungen für einen Betriebsartenwechsel definiert? Wo sind diese dokumentiert?**

Für die fehlersicheren Ein-/Ausgabemodule F-SM existiert nur eine Betriebsart.

- 6.6 Ist eine Trennung von Betriebs- und Sicherheitsfunktionen in der Software vorgesehen?
Wenn ja, wie erfolgt diese Trennung?**

Die fehlersicheren Ein-/Ausgabemodule F-SM können nur entweder ausschließlich für sicherheitsgerichtete oder für betriebliche Aufgaben eingesetzt werden. Eine Trennung von Funktionen ist daher nicht erforderlich.

6.7 Wie wird der Kontrollfluss gesteuert?

Der Kontrollfluss ist über Zustandsmaschinen gesteuert. Sie sind als Zustandsdiagramme mit Beschreibung der Übergangsbedingungen spezifiziert.

**6.8 Welche zeitlichen Randbedingungen wurden festgelegt?
Wo sind diese beschrieben?**

Die Reaktionszeit einer Sicherheitsfunktion kann in Abhängigkeit des Hard- und Softwareausbaus des Systems berechnet werden.

6.9.1 Kann nachgewiesen werden, dass das resultierende Verhalten in vorhersagbarer Weise allein von den sicherheitstechnisch wichtigen Funktionen der Komponente bestimmt wird (deterministisches Verhalten)?

Es sind keine betrieblichen Funktionen innerhalb eines sicherheitsgerichteten Ein-/Ausgabemoduls F-SM implementiert.

6.9.2 Ist die Unabhängigkeit vom verfahrenstechnischen Anlagenprozess bzw. der zugehörigen Signaltrajektorien für:

- Programmablauf
- Interruptbehandlung
- Arbeitsauslastung der Prozessoren
- Kommunikationsbelastung

sichergestellt?

Aufgrund des zyklischen Austausches von Telegrammen ist der Programmablauf unabhängig vom Prozess.

6.9.3 Erfolgt eine strikt zyklische Bearbeitung aller sicherheitskritischen Funktionen der Komponente?

Die Zykluszeit der sicherheitskritischen Funktionen richtet sich nach dem DP-Buszyklus (vgl. 2.14) und ist somit strikt zyklisch.

6.9.4 Ist die mögliche Variationsbreite in der Programmlaufzeit gering und sind die beeinflussenden Faktoren beschrieben?

Die Programmlaufzeit richtet sich nach der Zykluszeit und ist immer konstant.

**6.10.1 Wird ein Betriebssystem verwendet? Wenn ja, welches?
Garantiert der Hersteller ein definiertes Zeitverhalten (Echtzeitbetriebssystem)?
Verfügt das Betriebssystem über erweiterte Sicherheitsfunktionen?**

Es wird kein Betriebssystem verwendet.

6.10.2 Sind im Betriebssystem oder der Anwendersoftware Überwachungsmechanismen für den Zugriff auf Speicherbereiche implementiert?

Wenn ja, wo sind diese beschrieben?

Nein

6.11 Welche Festlegungen zum Interrupthandling gibt es (Prioritäten etc.)? Wo sind diese dokumentiert?

Es werden nur Timerinterrupts zum zyklischen Aufruf verwendet.

6.12 Wurde vorgefertigte Software eingesetzt?, Wenn ja, wie wurde deren Zuverlässigkeit nachgewiesen?

Es wurde keine vorgefertigte Software eingesetzt.

7 Maßnahmen zur Fehlererkennung und Fehlerbeherrschung

7.1 Welche (Selbst-) Überwachungsfunktionen für die ordnungsgemäße Funktion der rechnergestützten Komponente sind implementiert? Wo sind diese detailliert beschrieben?

Im Sicherheitsbetrieb werden die Daten zwischen F-CPU und F-Peripherie in einem Sicherheitstelegramm gemäß PROFIsafe-Protokoll übertragen.

Die zeitliche Überwachung der Telegrammaktualisierung im PROFIsafe-Protokoll erfolgt durch eine fortlaufende Sequenznummer. Innerhalb einer parametrierbaren Überwachungszeit muss ein gültiges Sicherheitstelegramm mit einer gültigen Sequenznummer angekommen sein. Wenn innerhalb der Überwachungszeit kein Telegramm mit gültiger Sequenznummer erkannt wird, dann wird die F-Peripherie passiviert (vgl. 7.6.1).

Die Gültigkeit der im Sicherheitstelegramm enthaltenen Prozesswerte, die Korrektheit der zugeordneten Adressbeziehungen und die sicherheitsrelevanten Parameter werden über einen im Sicherheitstelegramm enthaltenen Prüfwert CRC abgesichert. Tritt ein Prüfwert-Fehler bei der Kommunikation zwischen F-CPU und F-Peripherie auf, z. B. durch eine elektromagnetische Störung, dann werden die nachfolgenden Wiederholungstelegramme ausgewertet, bis ein fehlerfreies Telegramm erkannt wird. Kann bis zum Ablauf des Watchdogtimers kein fehlerfreies Telegramm erkannt werden, wird die F-Peripherie passiviert.

Die Erzeugung der Telegramme erfolgt durch 2 redundante Mikrocontroller auf den fehlersicheren E/A-Baugruppen: einer erzeugt den Telegrammdateininhalt, der zweite erzeugt den CRC-Prüfwert.

7.2.1 Werden die Speicherbereiche, die den Programmcode oder unveränderliche Daten enthalten, überwacht? Wenn ja, auf welche Weise und wo ist dies dokumentiert?

Es erfolgt eine gegenseitige Überwachung der zwei redundanten Mikrocontroller für den Flash-Speicher und die identischen Teile des RAM. Nicht vergleichbare Speicherbereiche weisen eine doppelte Speicherung der Daten auf.

7.2.2 Gibt es Speicherzugriffsüberwachungen (z. B. hinsichtlich Feldindizes)?

Hierzu sind Assertions in das Programm integriert.

7.3.1 Erfolgt eine Prüfung der Eingangs- und Ausgangsdaten auf Einhaltung des Wertebereichs?

Hierzu sind in den vorliegenden Unterlagen keine Angaben enthalten.

7.3.2 Erfolgt eine Prüfung der Zwischenwerte auf zulässige Wertebereiche?

Hierzu sind Assertions in das Programm integriert.

7.3.3 Gibt es eine Überwachung hinsichtlich der Einhaltung der Wertebereiche der Modulein- und -ausgabewerte?

Hierzu sind in den vorliegenden Unterlagen keine Angaben enthalten.

7.4 Gibt es Überwachungsfunktionen für komponenteninterne Busfunktionen? Wenn ja, wo sind diese dokumentiert?

Die sicherheitsgerichteten Ein-/Ausgabemodule F-SM besitzen keine internen Busfunktionen. Sämtliche interne und externe Buskommunikation innerhalb des Integrated Safety Systems wird mit dem fehlersicheren Busprotokoll PROFIsafe abgewickelt.

7.5 Erfolgt eine Überwachung des Datenverkehrs über die Datenschnittstellen? Wenn ja, wo ist dies dokumentiert?

Fehler auf dem PROFIBUS DP bei der Übertragung sicherheitsrelevanter Nachrichten werden entsprechend IEC 61508 durch folgende Maßnahmen erkannt:

- Datenverfälschung: durch zusätzliche Sicherheitsinformationen in einer auf den Standard-PROFIBUS aufgesetzten Sicherungsschicht (PROFIsafe-Protokoll)
- Verlust, Verzögerung: Erkennung durch Zeitüberwachung
- Falsche Reihenfolge/Abfolge/Wiederholung: Erkennung durch Nummerierung der Telegramme
- Wiederholung und Einfügung: Erkennung durch logische Programmüberwachung und Nummerierung der Nachrichten
- Unterscheidung von sicherheitsrelevanten und nicht-sicherheitsrelevanten Nachrichten durch die zusätzliche Sicherungsschicht.

Die Überwachungsfunktionen sind in der Beschreibung (Draft) des PROFIsafe-Treibers "PROFIsafe - Profile for Safety Technology on PROFIBUS DP and PROFINET IO" enthalten.

7.6.1 Welches Fehlerverhalten hat die Komponente?

Grundlage des Sicherheitskonzeptes ist es, dass für alle Prozessgrößen ein sicherer Zustand existiert. Bei digitalen Signalbaugruppen ist das z. B. der Wert "0". Für eine fehlersichere Signalbaugruppe werden in folgenden Fällen statt der Prozesswerte automatisch Ersatzwerte, die dem sicheren Zustand entsprechen, ausgegeben (Passivierung der fehlersicheren Signalbaugruppe):

- beim Anlauf des F-Systems
- bei Fehlern in der sicherheitsgerichteten Kommunikation zwischen F-CPU und F-SM über das Sicherheitsprotokoll gemäß PROFIsafe (Kommunikationsfehler)

Ein Ausfall der zentralen Steuerung äußert sich als Kommunikationsfehler. Auch in diesem Fall geht die fehlersichere Signalbaugruppe in den sicheren Zustand.

7.6.2 Wie verhält sich die Komponente bei Störungen in der Stromversorgung?

Bei Stromausfall und damit einhergehendem Stopp der CPU werden die Ein- / Ausgabemodule F-SM in den passiven Zustand versetzt (vgl. 7.6.1).

**7.7 Gibt es eine Protokollierung bei Störungen oder Fehlern im Gerät?
Wenn ja, wie erfolgt diese Protokollierung?**

Erkannte Fehler werden in den Diagnosepuffer der F-SM und den Diagnosepuffer der CPU eingetragen und dem Sicherheitsprogramm in der F-CPU mitgeteilt.

8 Schnittstellen

8.1 Welche systeminternen und externen Schnittstellen hat das Gerät?

Das sicherheitsgerichtete Ein-/Ausgabemodul F-SM besitzt zu Kommunikationszwecken mit der CPU eine Rückwandbusanschlutung für die dezentrale Peripherie ET 200M, basierend auf dem PROFIsafe-Busprotokoll. Die ET 200M ist über PROFIBUS DP an die CPU angebunden.

8.2 Wie ist das implementierte Verhaltensmuster des Geräts / Systems an den Datenschnittstellen?

Siehe Angaben in den Kapiteln 2 und 7.

8.3 Was kann über die vorhandenen Schnittstellen an den Einrichtungen verändert werden (Parameter, Firmware)?

Die fehlersicheren Signalbaugruppen werden wie Standardbaugruppen mit STEP 7 HW Konfig über die MPI-Schnittstelle der CPU konfiguriert. Die Parameter werden beim Laden vom Programmiergerät (PG) in die F-CPU übertragen, dort gespeichert und von der F-CPU an die fehlersichere Signalbaugruppe übergeben.

Die fehlersichere Buskommunikation ist in einem von der CPU nicht änderbaren Systemprogramm realisiert (Flash).

8.4.1 Welche Mechanismen zum Schutz des Programmcodes und der Parameterdaten gegen unbeabsichtigte oder unbefugte Änderungen im Betrieb wurden implementiert?

Der Zugriffsschutz auf F-Systeme wird realisiert durch die Vergabe von Passwörtern für die F-CPU und für das Sicherheitsprogramm. Die Realisierung des Zugriffsschutzes ist ausführlich beschrieben.

- für S7 Distributed Safety im Handbuch "S7 Distributed Safety, Projektieren und Programmieren",
- für S7 F/FH Systems im Handbuch "Automatisierungssysteme S7 F/FH".

Programmänderungen an der F-CPU haben keine Auswirkungen auf die Funktionalität der sicherheitsgerichteten Buskommunikation, da diese als Systemprogramm unabhängig von den Anwendungsprogrammen realisiert ist und durch den Anwendungsprogrammierer nicht verändert werden kann. Eine Ausnahme hierzu stellt die Watchdogzeit für die Überwachung der Kommunikation dar, die als Parameter geändert werden kann.

8.4.2 Welches Verhalten zeigt die Komponente während der Parametrierung oder des Prüfens bzw. der Online-Diagnose?

Das Laden des gesamten F-Programms ist nur in der Betriebsart "STOPP" möglich. Diese Betriebsart muss durch einen Schalter an der Zentraleinheit des S7 F/FH-Systems eingestellt werden. Alle Ausgänge werden passiviert und erst durch die Rückstellung des Betriebsartenschalters wird das System wieder aktiviert.

Änderungen an der Software des F-Programms können sowohl in der Betriebsart "STOPP" also auch in "RUN" bzw. "RUN-P" durchgeführt werden. Für Änderungen im laufenden Betrieb (Betriebsartenschalter auf "RUN" bzw. "RUN-P") muss der Sicherheitsbetrieb der CPU deaktiviert werden, d. h. alle Sicherheitsmechanismen zur Fehlererkennung und Fehlerreaktion werden außer Kraft gesetzt. Dies erfolgt gesichert über ein Passwort (CPU-Passwort) vom Programmiergerät (PG) aus. Nach dem Änderungsladen muss der Sicherheitsbetrieb wieder aktiviert werden, um einen gesicherten Ablauf des F-Programms zu gewährleisten.

8.4.3 Muss die Komponente nach der Parametrierung oder Prüfung von Hand aus dem Parametrier- oder Prüfmodus wieder in den Betriebsmodus umgeschaltet werden oder erfolgt dies automatisch?

Nach dem Programmladen bzw. einer Parametrierung im Offline-Modus (Betriebsart STOPP) muss die CPU von Hand mit dem Betriebsartenschalter wieder gestartet werden (Betriebsart RUN). Bei Anlagenänderungen im laufenden Betrieb erfolgt die Wiederaufnahme des Standardbetriebs durch Wiederaufnahme des Sicherheitsbetriebes. Dieser wird mit dem Programmiergerät (PG), nach der Eingabe des CPU-Passwortes, wieder aktiviert.

8.6 Verfügt der eingesetzte Mikrokontroller über eine Bootstraploader-Funktionalität?

Wenn ja, wann und zu welchem Zweck wird er eingesetzt und in welchem Modus wird er betrieben und wo ist dies beschrieben?

Eine Bootstraploader-Funktionalität wird nicht bereitgestellt.

8.7 Wurde die Mensch-Maschine-Schnittstelle nach bestimmten Regeln aufgebaut?

Es ist keine Mensch-Maschine-Schnittstelle vorhanden.

8.8 Wurden für die Analogeingänge der Komponente geeignete Filter in der Hard- oder Software vorgesehen?

Für Interface-Baugruppen nicht relevant.

8.9 Wurden Maßnahmen für die zeitrichtige Behandlung von Binärsignalen getroffen?

Für Interface-Baugruppen nicht relevant.

8.10 Welche Maßnahmen wurden für die binären Eingänge getroffen um technologisch bedingte unerwünschte Signalwechsel (wie Kontaktprellen) zu behandeln?

Für Interface-Baugruppen nicht relevant.

9 Spezielle Fragen zu Interface-Baugruppen

9.1.1 Welche Netztopologien sind möglich?

Die Ein-/Ausgabemodule F-SM werden linienförmig über ein Buskabel miteinander verbunden. Die Zentralen des Integrated Safety Systems (F-CPU's) werden ringförmig miteinander vernetzt.

9.1.2 Sind redundante Busstrukturen möglich?

Mit Siemens SIMATIC S7 F/FH Systems können neben der Zentrale auch die Busverbindungen und die dezentralen Ein-/Ausgabemodule redundant ausgelegt und damit die Verfügbarkeit des Systems verbessert werden.

9.1.3 Ist ein Mischbetrieb mit nicht-sicherheitsgerichteten Nachrichten auf einer Kommunikationsverbindung möglich?

Wie wird die gegenseitige Beeinflussung sicherheitsrelevanter und nicht sicherheitsrelevanter Nachrichten verhindert?

Ein Mischbetrieb ist möglich. Die Unterscheidung zwischen sicherheitsgerichteten und konventionellen Nachrichten erfolgt durch eine zusätzliche Sicherungsschicht im ISO/OSI Schichtenmodell.

9.2.1 Ist eine Übertragung über Lichtwellenleiter (LWL) möglich?

Da die Kommunikation zwischen den Busteilnehmern über den Industriestandard PROFIBUS DP läuft, können beliebige Medien zur Übertragung eingesetzt werden.

9.2.2 Können konventionelle Netzwerkkomponenten für den Aufbau der Netztopologie verwendet werden?

Aufgrund des Grey-Channel Prinzips ist keine spezielle Hardware notwendig (Standard-PROFIBUS Hardware).

9.2.3 Welche Verbreitung hat die Komponente in der Industrie?

Eine Vielzahl von Geräten sind auf dem Markt erhältlich. Die Systeme Siemens Distributed Safety und Siemens S7 F/FH Systems sind bereits langjährig im Einsatz. Die meisten Peripheriekomponentenhersteller (z. B. WAGO, B&R) liefern Komponenten mit eingebauten PROFIsafe Interface.

9.3.1 Ist die direkte Kommunikation von peripheren Busteilnehmern ohne Sicherheitszentrale möglich?

Nein, da ein Master/Slave basiertes System vorliegt.

9.3.2 Welches Konzept liegt dem sicherheitsgerichteten Bussystem zugrunde?

Das Konzept des sicherheitsgerichteten Bussystems basiert auf einer zusätzlich zum Standard-PROFIBUS DP-Protokoll realisierten softwarebasierten Sicherungsschicht im ISO/OSI-Schichtenmodell.

9.3.3 Welches Buszugriffsverfahren wird verwendet?

Es wird eine Master/Slave-Kommunikation mit Polling-Verfahren verwendet, die zu einer kontrollierten, deterministischen Kommunikation führt.

9.3.4 Können die Nachrichten mit Prioritäten versehen werden?

Da die Abarbeitung der Busteilnehmer streng zyklisch ist, ist zur Einhaltung der Reaktionszeiten eine Priorisierung nicht erforderlich.

9.3.5 Wie ist das Verhalten des Bussystems bezüglich der Reaktionszeit?

Der Buszugriff erfolgt streng zyklisch. Der Master fragt nacheinander die Slaves ab. Die Reaktionszeit ist im fehlerfreien Fall und im Fehlerfall genau vorhersagbar.

9.3.6 Ist die der Baugruppe zugrunde liegende Protokollspezifikation herstellereinspezifisch oder ein offengelegtes Protokoll?

PROFIsafe ist ein offenes System der Siemens AG bzw. der PROFIBUS Nutzerorganisation (PNO). Es ist im industriellen Bereich weit verbreitet.

9.3.7 Wie groß ist die Hamming-Distanz der Datenübertragung auf dem Bussystem?

Die Hamming-Distanz ist 4, d. h. bis zu 3 Bitfehler können erkannt und korrigiert werden.

9.4.1 Werden die typischen Fehler für Buskommunikation (Verlust, Wiederholung, Einfügung, falsche Abfolge, Verzögerung und Nachrichtenverfälschung) beherrscht? Welche Maßnahmen werden bei Fehlererkennung ergriffen?

Die Fehlertypen werden beherrscht durch

- eine fortlaufende Nummerierung der Sicherheitstelegramme
- eine Zeiterwartung für den Abstand ankommender Telegramme bzw. deren Quittierung
- eine Kennung zwischen Sender und Empfänger ("Lösungswort")
- eine zusätzliche Datensicherung (CRC)

Die zusätzlichen Telegrammbestandteile werden in den Nutzdaten des Standard-Telegramms durch eine Softwareschicht oberhalb der DP-Layer-Software integriert.

9.4.2 Wie wirkt sich der Ausfall einzelner Busteilnehmer auf das Netzwerk aus?

Da die Busteilnehmer zyklisch von der Zentrale abgefragt werden und diese den Ausfall eines Teilnehmers erkennt und ihn über definierte Fehlerreaktionen kompensieren kann, ergeben sich keine Auswirkungen auf das Netzwerk.

9.4.3 Wird ein Watchdog verwendet?

Eine Überwachung der Telegrammabstände durch einen Watchdog findet statt.



Anhang II: Ausgefüllter Fragenkatalog Typvertreter II

Inhalt:

Fragenkatalog zum Typvertreter II (CANopen Safety Chip) mit 28 Seiten

1 Projektplanung und Aufbau der Dokumentation

1.1.1 Welches Vorgehensmodell wurde der Entwicklung zugrunde gelegt (z. B. Verfahrens-Modell, V-Modell)?

Aus den angegebenen Entwicklungsdokumenten kann ein phasenorientiertes Vorgehensmodell abgeleitet werden.

1.1.2 Gibt es eine Liste sämtlicher, entsprechend den Phasen des Vorgehensmodells, geordneter Dokumente?

Folgende Entwicklungsdokumentation wurde erstellt:

- Masterdokument
- Produkthanforderungen
- Sicherheitskonzept
- Hardwaredesign
- Softwaredesign
- Technische Dokumentation und Nutzerhandbuch
- Verifikations- und Validationsplan
- Hardwareprüftest und Hardwareprüfergebnisse
- Softwareprüftest und Softwareprüfergebnisse
- Übersicht Op-Code und Adressierungen
- Schaltplan

1.1.3 Sind die einzelnen Phasen des Lebenszyklus des Produktes und die zugehörigen Aktivitäten detailliert festgelegt?

Hierzu sind in den vorliegenden Unterlagen keine Angaben enthalten.

1.1.4 Gibt es einen produktspezifischen Projektplan? Wenn ja, was wurde dort festgelegt?

Hierzu sind in den vorliegenden Unterlagen keine Angaben enthalten.

1.1.5 Gibt es einen produktspezifischen Qualitätssicherungsplan (oder -konzept) oder ein vergleichbares Dokument?

Die Firma SYSTEC electronic GmbH besitzt ein allgemeines Qualitätsmanagementsystem nach DIN EN ISO 9001:2000. Der Entwicklung wurden die Arbeitsanweisungen "Entwicklung" und "Richtlinien zur Softwareimplementierung" zugrunde gelegt. Hinsichtlich eines produktspezifischen Qualitätssicherungsplanes werden keine Angaben gemacht.

1.1.6 Gibt es Festlegungen zu den verantwortlichen Personen, Abteilungen und Organisationen für jede Phase des Lebenszyklusses?

Wurden insbesondere Verifikations- und Validierungsaufgaben von den Implementierungsaufgaben getrennt?

Hierzu sind in den vorliegenden Unterlagen keine Angaben enthalten. Durch die Typprüfung des TÜV Rheinlands erfolgte eine herstellerunabhängige Prüfung.

1.1.7 Unterliegen die relevanten Dokumente hinsichtlich ihrer Überarbeitung, Prüfung und Freigabe einem angemessenen System der Dokumentenlenkung?

Aus den Standardangaben auf den Dokumentenblättern ist eine anforderungsgerechte Dokumentenlenkung gemäß DIN EN ISO 9001:2000 erkennbar.

1.2.1 Gibt es eine Anforderungsspezifikation (Lastenheft)?

Wenn ja, sind dort

**Funktionsanforderungen,
Sicherheitsanforderungen,
Normen die der Entwicklung bzw. Qualifizierung zugrunde gelegt
wurden**

enthalten?

Es existiert die Anforderungsspezifikation "Produktanforderungen". Sie enthält Funktionsanforderungen, Sicherheitsanforderungen, Umgebungsbedingungen, zeitliche Programmlaufanforderungen sowie Anforderungen von Seiten des CANopen Protokolls. Normen die der Entwicklung und Qualifizierung zugrunde lagen werden, nicht aufgeführt.

Normen, die der Qualifizierung zugrunde lagen werden im Prüfbericht "Bericht über die Prüfung des CANopen Safety Chip CSC01" aufgeführt.

1.2.2 Gibt es eine Systemspezifikation (Pflichtenheft, Entwurfsspezifikation) für Hardware und Software?

Als Systemspezifikation existiert das Dokument "Sicherheitskonzept".

1.2.3 Wie ist die Entwicklungsdokumentation aufgebaut?

Teile der Entwicklungsdokumentation sind:

- Hardwaredesign
- Softwaredesign
- Übersicht Op-Code und Adressierungen (lag nicht vor)
- Schaltplan (lag nicht vor)

**1.2.4 Gibt es eine Prüfspezifikation für die Komponente?
Wie ist die Prüfdokumentation aufgebaut?**

Es existieren folgende Prüfspezifikationen:

- Verifikations- und Validierungsplan
- Hardwareprüftest und Hardwareprüfergebnisse
- Softwareprüftest und Softwareprüfergebnisse

Sie enthalten Angaben zu den einzelnen Prüfungen, der Prüfumgebung, den Prüfwerkzeugen, den Prüffällen, den Prüfkriterien und der Prüfkongfiguration. Es werden Softwaretests, Hardwaretests sowie Hardware-/Softwareintegrationstests beschrieben.

1.2.5 Können die kompletten Softwarequellen (Sourcecode) vorgelegt werden?

Die Firmware lag bei der Typprüfung mit dem TÜV-Prüfbericht "Bericht über die Prüfung des CANopen Safety Chip CSC01", Bericht-Nr.: 968/EL 215.01/04 vom 30.07.2004 vor.

1.3.1 Gibt es detaillierte Festlegungen zum Konfigurations- und Änderungsmanagement für die Hard- und Software? Wenn ja, wo ist diese dokumentiert?

Es werden keine Angaben zu einem Konfigurations- und Änderungsmanagement für die Hard- und Software gemacht, außer der Verwendung des Werkzeugs WinCVS (Concurrent Versions System). Dieses Programm stellt eine Versionskontrolle und ein Änderungsmanagement für die Software zur Verfügung. Die Verwendung von WinCVS stellt eine Kontrolle und Dokumentation der Konfiguration und Änderungen sicher.

1.3.2 Gibt es ein KID (Konfigurations-Identifikations-Dokument)?

Hierzu sind in den vorliegenden Unterlagen keine Angaben enthalten.

1.4 Welche Normen wurden der Entwicklung zugrunde gelegt?

Im Rahmen der Typprüfung wurde die Einhaltung folgender Normen und Richtlinien geprüft:

IEC 61508 Part 1 - 7

Functional safety of electrical/electronic/programmable electronic safety-related systems

DIN EN 954-1/03.97

Sicherheit von Maschinen, Sicherheitsbezogene Teile von Steuerungen
Teil 1: Allgemeine Gestaltungsleitsätze

Grundsatz für die Prüfung und Zertifizierung von "Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten", Hauptverband der gewerblichen Berufsgenossenschaften, Fachausschuss Elektrotechnik, Köln, Ausgabe 05.02, GS-ET-26

2 Funktionen und Auslegungsvorgaben unter Sicherheitsaspekten**2.1 Gibt es eine detaillierte Beschreibung der Leittechnik-, Überwachungs- und Unterstützungsfunktionen, die für nicht an der Entwicklung beteiligte Personen nachvollziehbar ist?**

Ja, in Form des Dokuments "Sicherheitskonzept".

2.2 Gibt es eine detaillierte Beschreibung der Aufgaben und Funktionen, die die Software zu erfüllen hat, die für nicht an der Entwicklung beteiligte Personen nachvollziehbar ist?

Die Softwaredokumentation des CSC01 entspricht den Anforderungen der IEC 61508. Die Struktur ist angelehnt an das Dokument der Prüfstelle "Requested documents for a development accompanying assessment and type approval according to IEC 61508". Das Dokument genügt gemäß Typprüfbericht den formalen und inhaltlichen Ansprüchen und ist nachvollziehbar.

2.3 Gibt es eine detaillierte Beschreibung der Konfigurations- und Parametriermöglichkeiten?

Das Dokument "Technische Dokumentation und Nutzerhandbuch" in der Version 1.06 wurde vom TÜV Rheinland im Zusammenhang mit der Zertifizierung inspiziert. Es enthält die für die richtige sicherheitstechnische Verwendung des CSC01 durch einen Anwender/Entwickler notwendigen Informationen.

2.4 Gibt es mehrere Varianten der Komponente (z. B. eine Sondervariante für den sicherheitstechnischen Einsatz)? Wenn ja, wie unterscheiden sich diese hinsichtlich Hard- und Software voneinander?

Es existiert nur eine Variante des CSC01. Nicht sicherheitsgerichtete CAN-Interfaces basieren ebenfalls auf dem M306NAFGTFP der Firma Renesas

2.5 Gab es eine Entwicklungsvorgabe, dass Betriebs- und sicherheitstechnisch wichtige Funktionen unabhängig voneinander arbeiten müssen?

Ja. Sicherheitstechnische Funktionen sind in der fest eingebetteten Firmware enthalten. Nicht-sicherheitstechnische Funktionen können in der Applikationssoftware hinzugefügt werden. Die Überwachung dieser Funktionen liegt in der Verantwortung des Anwendungsherstellers. Die beiden Programmbereiche sind voneinander getrennt und tauschen Daten über Shared-Memory bzw. Puffer-Speicher aus.

2.6 Gab es Entwicklungsvorgaben hinsichtlich besonderer (Selbst-) Überwachungsfunktionen? Wenn ja, gibt es eine detaillierte Beschreibung dieser Funktionen?

Die Entwicklungsvorgaben resultieren aus der geforderten Qualifizierungsfähigkeit gemäß IEC 61508. Vor Beginn der Entwicklung wurde das Konzept durch den TÜV Rheinland überprüft.

Die Maßnahmen zur Fehlererkennung und -beherrschung wurden im Vorfeld der Zertifizierung nach IEC 61508 in einem Design Review vom TÜV Rheinland verifiziert (u. a. CPU, OP-Code, System Stack, Register, Interne Peripherie). Eine Diagnose des RAM erfolgt mit einem Galpat-Test, der sich alle 68 min wiederholt.

Eine detaillierte Beschreibung der Überwachungsfunktionen befindet sich in dem Dokument "Softwaredesign".

2.7 Gab es Entwicklungsvorgaben hinsichtlich fehlerbeherrschender Strukturen und Maßnahmen (z. B. Fail-Safe-Verhalten, fehlertoleranter Aufbau, Verhinderung unzulässiger Operationen)?

Die Entwicklungsvorgaben resultieren aus der geforderten Qualifizierungsfähigkeit gemäß IEC 61508. Vor Beginn der Entwicklung wurde das Konzept durch den TÜV Rheinland überprüft.

Der Mikrokontroller ist mit zwei redundanten CAN-Businterfaces ausgestattet.

Das CAN-Protokoll besitzt eine Hamming-Distanz von 6. Das bedeutet, dass durch Prüfsummen bis zu 5 Bitfehler korrigiert werden können. Ab 6 Bitfehlern kann der Fehler nur noch detektiert, nicht aber korrigiert werden. Durch diese sehr hohe Hamming-Distanz ist der CAN-Bus in hohem Maße fehlertolerant.

Wird der CSC01 in einer Aktoranwendung eingesetzt, so muss ein externer Watchdog mit eigener Zeitbasis und zweitem Abschaltpfad aufgebaut werden. Er überwacht den Programmablauf des CSC01. Die Datenkonsistenz des Speichers wird durch verschiedene Prüfroutinen (CRC, Galpat-Test) sichergestellt.

Bei fehlerhaftem Verhalten wird ein definierter Fehlerzustand (der sogenannte "sichere Zustand" in der IEC 61508 Terminologie) angefahren, d. h. die Buskommunikation wird eingestellt und die Ausgänge werden über eine Sicherheitsschalteneinrichtung abgeschaltet (vgl. 2.11).

Hinweis: Der Einsatz von gemäß IEC 61508 zertifizierten Geräten in der Industrie erfolgt grundsätzlich für sicherheitsgerichtete Funktionen, die einen eindeutigen Fail-Safe-Zustand (z. B. Maschinenabschaltung, Stromabschaltung, etc.) aufweisen.

2.8 Gab es Entwicklungsvorgaben zur Auslegung gegen besondere Umwelteinflüsse (EMV, induzierte Erschütterungen aus Erdbeben, KMV etc.)?

Die Auslegung gegen besondere Umwelteinflüsse liegt im Verantwortungsbereich des Geräteherstellers, der den Chip in eine Komponente integriert. Der Einsatztemperaturbereich des CSC01 beträgt -40°C bis +85°C.

2.9 Gab es Entwicklungsvorgaben hinsichtlich des Schutzes der gespeicherten Programme und Parameter gegen Veränderung?

Die Software besteht aus zwei Teilen. Die CANopen Safety Applikation wird von Gerätehersteller entwickelt und von ihm während der Produktion in den Flash programmiert. Dieser Teil der Software kann vom Gerätehersteller nicht verändert werden. Er wird im Produktionsprozess des CANopen Safety Chips in den Flash programmiert.

Um den Applikationsflash des Mitsubishi M306NAFGTFP zu programmieren, wird der Programmiermodus benötigt. Dieser Modus wird über den Bootjumper und einen Reset aktiviert. Nun kann mit entsprechenden Programmierertools der Microcontroller über die serielle Schnittstelle programmiert werden. Während der Programmierung muss der Bootjumper geschlossen bleiben. Der Zugriffsschutz der Anwendersoftware muss vom Applikationshersteller - z. B. durch Einbau des Chips in ein geschlossenes Gehäuse - bereitgestellt werden.

2.10 Gab es Entwicklungsvorgaben zu den Prinzipien zur Sicherstellung eines möglichst deterministischen Verhaltens (z. B. einer streng zyklischen Abarbeitung des Hauptprogrammes)?

Die Entwicklungsvorgaben resultieren aus der geforderten Qualifizierungsfähigkeit gemäß IEC 61508. Vor Beginn der Entwicklung wurde das Konzept durch den TÜV Rheinland überprüft.

Alle Nachrichten werden streng zyklisch gesendet, unabhängig von einer Anforderung durch das Applikationsprogramm. Der Abstand der Telegramme ist abhängig von der eingestellten SCT (Safeguard Cycle Time), die minimal 20 ms beträgt.

2.11 Gab es Entwicklungsvorgaben hinsichtlich des Ausfall- bzw. Fehlerverhaltens der Komponente?

Die Entwicklungsvorgaben resultieren aus der geforderten Qualifizierungsfähigkeit gemäß IEC 61508. Vor Beginn der Entwicklung wurde das Konzept durch den TÜV Rheinland überprüft.

Wird ein Diagnosefehler oder ein Fehler im CAN-Treiber festgestellt, so verweilt die Main-Funktion in einer Endlosschleife im Betriebszustand STOPP, dem "sicheren Zustand" gemäß IEC 61508. In diesem Zustand wird der Watchdog nicht mehr getriggert und die CAN-Kommunikation wird abgeschaltet. Alle Interrupts werden gesperrt. Da in diesem Zustand der Watchdog nicht mehr bedient wird, werden die Ausgänge eines Aktors über den zweiten Abschaltweg in den sicheren Zustand gesetzt.

2.12 Gab es Entwicklungsvorgaben, dass die Komponente (z. B. steckbare Baugruppe) bei Betrieb austauschbar ist?

Der CANopen Safety Chip ist für den Einbau in herstellerspezifische Applikationen vorgesehen. In der Applikation muss eine entsprechende Eigenschaft realisiert werden.

2.13 Gab es Entwicklungsvorgaben hinsichtlich einer energetischen, datentechnischen und funktionalen Entkopplung an den Schnittstellen zur Kraftwerksanlage (Fehlerfortpflanzungssperren)?

Die Anschaltung der Transmitterleitungen (CAN-Treiber) sind bei der späteren Geräteentwicklung über Dioden zu entkoppeln. Funktionale Entkopplung ist für informationstechnische Baugruppen nicht relevant.

Die streng zyklische Bearbeitung der Datentelegramme trägt zu der datentechnischen Entkopplung bei.

2.14 Gab es Entwicklungsvorgaben zur Sicherstellung von konstanten Betriebsbedingungen der Komponente (wie statische Zuordnung von Systemressourcen, so dass die Systemfunktionen unabhängig vom Prozess gleichbleibend beansprucht werden, zyklische Bearbeitung der Anwenderfunktionen, Verzicht auf prozessabhängige Interrupts, vorbeugende Maßnahmen gegen Software-Exceptions)?

Die Entwicklungsvorgaben resultieren aus der geforderten Qualifizierungsfähigkeit gemäß IEC 61508. Vor Beginn der Entwicklung wurde das Konzept durch den TÜV Rheinland überprüft.

Entwicklungsvorgaben gab es bezüglich der zyklischen Telegrammabarbeitung und -sendung. Daraus folgt, dass auch der sicherheitsgerichtete Programmteil des Mikrokontrollers zyklisch abgearbeitet wird. Ein externer Watchdog überwacht die Einhaltung der zyklischen Abarbeitung.

2.15 Gab es Entwicklungsvorgaben zur Performance (Zeitverhalten, zu berücksichtigende Belastungen, Anlaufverhalten, Genauigkeit, maximale Auslastung des Prozessors, zu erwartende Belastungen)?

Die resultierenden Reaktionszeiten sind abhängig von der eingestellten SCT (Safeguard Cycle Time), die minimal 20 ms beträgt. Die Verzögerungszeiten durch die interne Programmlaufzeit des CSC-Main Programms und des Applikationsprogramms betragen maximal 7 ms. Die Reaktionszeit des CSC01 ist damit maximal gleich der SCT + 7 ms. Die Abarbeitung des sicherheitsgerichteten Programmteils erfolgt streng zyklisch mit der eingestellten Safeguard Cycle Time.

2.16 Wurden verschiedene Betriebsarten definiert? Wenn ja, wo sind diese dokumentiert?

In den vorliegenden Unterlagen werden keine unterschiedlichen Betriebsarten beschrieben.

2.17 Wurde eine Gefährdungs- / Risikoanalyse für die Komponente durchgeführt?

Es wurde eine Gefährdungs-/Risikoanalyse im Rahmen der IEC 61508 Zertifizierung durchgeführt.

2.18 Wurden Maßnahmen getroffen, um die Lieferbarkeit der verwendeten Hardwarekomponenten dauerhaft sicherzustellen? Wenn ja, wie sehen diese aus?

Bei der Hardwareauswahl wurde in dem Dokument "Hardwaredesign" ein Nachfolgetyp des Mikrokontrollers berücksichtigt und seine grundsätzliche Nachfolgequalifizierung geprüft.

2.19 Wurden über die Spezifikationen hinausgehende verborgene Funktionalitäten implementiert, die im Entwicklungsprozess als erforderlich angesehen wurden (z. B. zu Entwicklungszwecken, zur Wartung und Diagnose)?

Hierzu sind in den vorliegenden Unterlagen keine Angaben enthalten.

2.20 Wie werden die systemimmanenten Eigenschaften der derzeit eingesetzten nicht digital ausgeführten Komponente bei der rechnergestützten Komponente abgebildet?

Derzeit werden festverdrahtete Verbindungen eingesetzt. Diese zeichnen sich durch verzögerungsfreie Übertragung und Parallelität aus. Bei der Verwendung eines Bussystems muss die von der Zykluszeit abhängige Verzögerung berücksichtigt werden. Aufgrund der bei CSC01 vorliegenden streng zyklischen Abarbeitung ist es möglich, die maximale Verzögerungszeit anzugeben. Diese muss bei der Systemauslegung berücksichtigt werden. Parallele Datenübertragung ist für mehrere Signale innerhalb eines Datenpaketes grundsätzlich möglich.

Der Einfluss von Einzelfehlern wirkt sich bei festverdrahteten Verbindungen jeweils nur auf ein Signal aus. Bei Bussystemen muss der gleichzeitige Ausfall einer Vielzahl von unterschiedlichen Signalen unterstellt werden.

Die Fehlerquellen Kurzschluss und Drahtbruch müssen bei festverdrahteten Verbindungen detektiert werden. Aufgrund der zyklischen Nachrichtenübertragung und der Watchdog-Überwachung werden derartige Ausfälle des Bus-Kabels erkannt. Die neu hinzukommenden Fehlertypen (Datenverfälschung, Verlust, Verzögerung, falsche Reihenfolge, Wiederholung) werden durch die Selbstüberwachungsfunktionen ebenfalls erkannt.

3 Analytische Maßnahmen zur Fehlervermeidung bei der Entwicklung

3.1 Wurde ein Prüfkonzert für die Komponente zugrunde gelegt? Wenn ja, enthält dieses Aussagen zu folgenden Fragestellungen:

Wann wird geprüft (z. B. Festlegungen zu Reviews)?

Was für Prüfmittel kommen zum Einsatz?

Wer führt die Prüfungen durch (Trennung Entwicklung /Test)?

Wie wurden die Prüfungen dokumentiert (Protokolle)?

Mit dem Dokument "Verifikations- und Validierungsplan" liegt ein Prüfkonzert für Soft- und Hardwaretests vor. Die Dokumentation der durchgeführten Tests erfolgt in den Dokumenten "Softwareprüftest und Softwareprüfergebnisse" sowie "Hardwareprüftest und Hardwareprüfergebnisse". Die Dokumentation wurde im Rahmen der Zertifizierung geprüft. Die Spezifikationen und Prüfprotokolle liegen vor.

Bei der Prüfung der Software kamen der Simulator der Entwicklungsumgebung und ein Bus-Analyser (CANalyser) zum Einsatz. Es wurde sowohl ein Test der einzelnen Software-Module als auch ein Integrationstest durchgeführt. Die Hardwareprüfung beschränkte sich auf die sicherheitstechnischen Komponenten, da die Hardware einen Prototyp darstellt.

3.2.1 Was für Typprüfungen wurden durchgeführt?

Wurden im Rahmen der Typprüfungen auch

- EMV-Prüfungen,
- Prüfungen der Auslegung gegen induzierte Erschütterung (Schwingen und Schocken),
- Prüfung zur Auslegung gegen besondere Umwelteinflüsse

durchgeführt?

Es wurde eine Typprüfung nach IEC 61508 durchgeführt. Gegenstand dieser Prüfung waren der Mikrokontroller und die zugehörige Software. Als Prüfling diente ein Prototyp in Form eines Evaluierungs-Boards. Im Rahmen der späteren applikationsspezifischen Entwicklungen müssen weitere Hardware-Belastungstests durchgeführt werden.

3.2.2 Wurden statische und dynamische Tests der Software durchgeführt?

Das dynamische Verhalten der Software wurde in Modul- und Integrationstests geprüft. Statische Tests des Codes erfolgten vermutlich im Rahmen der Zertifizierung nach IEC 61508.

3.2.3 Gibt es einen Softwaretestbericht mit Angaben zu den durchgeführten statischen und dynamischen Tests?

Der Softwaretestbericht "Softwareprüftest und Softwareprüfergebnisse" gibt Auskunft über die durchgeführten dynamischen Softwaretests. Statische Softwaretests fanden vermutlich im Rahmen der Zertifizierung nach IEC 61508 statt, werden jedoch nicht beschrieben.

3.2.4 Welche Hard- und Software-Integrationstests wurden durchgeführt?

Es wurden Hard- und Software-Integrationstests mit einem Evaluierungsboard durchgeführt. Die Hardware-Integrationstests umfassen die Schnittstellen (seriell, CAN), die Stromversorgung, den Watchdog sowie die Not- und Abschaltfunktionen. Im Verlauf der Software-Integrationstests werden die einzelnen Programmmodule getestet.

**3.2.5 Welche Systemtests bzw. Systemintegrationstests wurden durchgeführt?
Wie wurden diese dokumentiert?**

Die Tests wurden an einer Prototyp-Hardware (Evaluierungs-Board) durchgeführt. Hierbei wurden unter anderem Belastungstests, Zeitmessungen und Fehlerfälle geprüft. Dokumentiert werden sie im Softwaretestbericht "Softwareprüftest und Softwareprüfergebnisse".

3.3.1 Wurden die Ablaufreihenfolge, die Aufruf- und Anlaufbedingungen der Tasks überprüft?

Es wurde keine Aufteilung in mehrere Tasks vorgenommen.

3.3.2 Wurden spezielle Werkzeuge oder automatische Testhilfen für die Prüfung der Software eingesetzt? Wenn ja, welche?

Die eingesetzten Werkzeuge sind:

- CANalyser
- Entwicklungsumgebung Tasking Tools für M16C v2.3 (Debugger, Simulator)

3.3.3 Wurden Tests der Software in einer Emulationsumgebung durchgeführt (z. B. Softwareemulation, In-Circuit-Emulation (ICE))?

Wurde der Programmcode so instrumentiert, dass während der Testphasen Tracing-Informationen gewonnen werden können?

Es wurden Tests der Softwaremodule innerhalb der Entwicklungsumgebung durchgeführt.

3.3.4 Wurden Simulations-Tools zur Prüfung der Software oder im Rahmen der Systemtests eingesetzt?

Es kam der Simulator, der Teil der Entwicklungsumgebung ist, zum Einsatz.

3.3.5 Wurde eine Timing-Analyse durchgeführt?

Das Zeitverhalten der Nachrichten auf dem CAN-Bus wurde mit dem Vector CANalyser und der dazugehörigen CANcardX ermittelt.

3.3.6 Erfolgte eine Überprüfung der Datenraten, Reaktionszeiten und des Verhaltens in Grenzsituationen (Performanceprüfungen)?

Im Dokument "Softwareprüftest und Softwareprüfergebnisse", wird eine ausführliche Prüfung des Zeitverhaltens der Software durchgeführt (z. B. Ermittlung maximaler Durchlaufzeiten und Belastungstests).

**3.3.7 Welche Validierungsprüfungen wurden durchgeführt?
Wurden insbesondere Maßnahmen zur Validierung von automatisch
durch Werkzeuge erzeugte Software getroffen?**

Es wurden Integrationstests von Software und Evaluierungsboard durchgeführt. Automatisch durch Werkzeuge erzeugte Software kommt nicht zum Einsatz.

**3.3.8 Wurden Prüfungen der (Mikrokontroller-)Hardware vor der HW/SW-
Integration durchgeführt?**

Der Test der Prototyp-Hardware erfolgt nach den Vorgaben im Dokument "Hardwareprüftest und Ergebnisse". Da es sich bei der Hardware um einen Prototypen bzw. eine Entwicklungsplattform handelt, die nicht in Endgeräten eingesetzt wird, wurde der Aufwand für die Prüfung und die Verifikation auf die sicherheitsrelevanten Komponenten beschränkt.

**3.3.9 Erfolgte eine Überprüfung der Auslastung des Speichers und des
Stacks?**

Hierzu sind in den vorliegenden Unterlagen keine Angaben enthalten.

**3.4 Wurde ein Verfahren festgelegt, wie mit festgestellten Fehlern
umgegangen wird (z. B. Einteilung in Fehlerklassen)? Wenn ja, wo ist
dieses dokumentiert?**

Zu den Verfahren sind in den vorliegenden Unterlagen keine Angaben enthalten. Die im Rahmen der Tests erkannten Fehler sind in der Prüfdokumentation beschrieben.

**3.5.1 Wurden spezielle methodische Verfahren zur Analyse möglicher
Störungen, Fehler oder Ausfälle für die Komponente ggf. auf der
Bauteil-/ Einzelkomponentenebene durchgeführt (z. B. FTA, FMEA)?**

Eine Fehlerbetrachtung erfolgte im Rahmen der Zertifizierung gemäß IEC 61508.

**3.5.2 Gab es Untersuchungen der Hard- und Software hinsichtlich des CCF
(Common-Cause-Failure)-Potentials?**

Hierzu werden in den vorliegenden Unterlagen keine expliziten Angaben gemacht.

Spezifisch für Interfaces sind hierbei Fehler auf dem Bus, sowie die Fehlerfortpflanzung von der Sender- auf die Empfangsseite zu betrachten. Gemäß Anhang B der IEC 61508-2 werden für zertifizierte Geräte bezüglich der systematischen Ausfälle fehlervermeidende Maßnahmen und Maßnahmen zur Beherrschung von Ausfällen getroffen. Dies bildet sich auch in den entsprechenden Kapiteln des vorliegenden Fragenkataloges ab (Kapitel 3, 5 und 6 bzw. Kapitel 7).

4 Betrieb und Wartung, wiederkehrende Prüfungen

4.1 Gibt es einen Prüfmodus für Inbetriebsetzung und wiederkehrende Prüfungen (WKP)?

Nicht relevant für Interface-Baugruppen.

4.2 Welche Dokumentationsunterlagen gibt es für den Benutzer und den Service?

Gibt es

- ein Benutzerhandbuch?
- eine Bedienungsanleitung?
- eine Reparaturanleitung?
- eine Konfigurationsanleitung?
- Prüfanweisungen?

Folgende Dokumentationsunterlagen existieren:

- Technische Dokumentation und Nutzerhandbuch

4.3 Welche Festlegungen für den Benutzer gibt es, wenn während des Betriebes Abweichungen (Fehlermeldungen) auftreten?

Nicht relevant für Interface-Baugruppen.

4.4.1 Sind eine größere Anzahl identischer Komponenten unter vergleichbaren Einsatzbedingungen bereits über einen längeren Zeitraum eingesetzt?

Der CSC01-Chip ist eine Neuentwicklung. Der verwendete Mikrokontroller M306NAFGTFP wird seit dem Jahr 2000 in großen Stückzahlen in der Serienfertigung im Automotive Bereich eingesetzt.

Vorliegende Zahlen:

- Autoradios: ca. 35.000 Stück/Monat
- Multifunktionslenkrad: ca. 20.000 Stück/Monat
- Lenksäulenmodul: ca. 15.000 Stück/Monat seit Anfang 2002
- Zusatzheizung: ca. 10.000 Stück/Monat seit Anfang 2001

4.4.2 Wurden besondere Möglichkeiten zur Gewinnung von Betriebsdaten oder Diagnosedaten vorgesehen?

Hierzu sind in den vorliegenden Unterlagen keine Angaben enthalten.

4.4.3 Wurden die bisherigen Betriebserfahrungen mit der Komponente systematisch erfasst und nachvollziehbar und vertrauenswürdig dokumentiert?

Da es sich um eine Neuentwicklung handelt hier nicht relevant.

4.4.4 Sind Ausfälle der Komponente bekannt? Wenn ja, wurden die Ursachen für Ausfälle der Komponente eingehend untersucht und dokumentiert?

Da es sich um eine Neuentwicklung handelt hier nicht relevant.

4.4.5 Werden die sicherheitstechnisch wichtigen Funktionen der Komponente regelmäßig innerhalb eines kurzen Zeitintervalls angefordert?

Durch die Verwendung als Businterface mit zyklischer Datenübertragung ist eine ständige Anforderung gegeben.

5 Konstruktive Maßnahmen zur Fehlervermeidung bei der Hardwareentwicklung

5.1 Gibt es eine detaillierte Beschreibung der Hardware mit Angaben zur Struktur, Modularisierung etc., die für nicht an der Entwicklung beteiligte Personen nachvollziehbar ist?

Die Hardwaredokumentation des CSC01 entspricht den Anforderungen der IEC 61508. Die Struktur ist angelehnt an das Dokument der Prüfstelle "Requested documents for a development accompanying assessment and type approval according to IEC 61508". Das Dokument genügt den formalen und inhaltlichen Ansprüchen für die Zertifizierung und ist nachvollziehbar.

5.2 Welcher Mikrokontroller bzw. Mikroprozessor (Hersteller, Typ) wurde ausgewählt und was waren die Kriterien für die Auswahl?

Der CSC01 basiert auf dem 16-Bit-Mikrocontroller M306NAFGTFP Step D der Firma Renesas.

Der Mikrokontroller ist eine Single Chip Ausführung mit zwei, räumlich separierten, integrierten CAN-Kontrollern. Er wird seit dem Jahr 2000 in großen Stückzahlen in der Serienfertigung im Automotive Bereich eingesetzt.

Vorliegende Zahlen:

- Autoradios: ca. 35.000 Stück/Monat
- Multifunktionslenkrad: ca. 20.000 Stück/Monat
- Lenksäulenmodul: ca. 15.000 Stück/Monat seit Anfang 2002
- Zusatzheizung: ca. 10.000 Stück/Monat seit Anfang 2001

5.3 Wie ist die Speicherorganisation der Komponente (von Neumann, (mod.) Harvard-Struktur) und wie erfolgt die Trennung von Daten und Programmen?

Es werden keine Angaben zur Speicherorganisation gemacht.
Die Programme werden in einem Flash-Speicher abgelegt, Daten im RAM.
Es erfolgte eine Einteilung in verschiedene Speicherbereiche, die verschiedenen Funktionen/Daten zugeordnet sind.

5.4 Welche Programm- und Datenspeicher (Typ, Größe ...) sind eingesetzt? Wo ist dies dokumentiert?

Der Chip besitzt 10 kByte internes SRAM und 256 kByte Flash-Memory.

Bereits beim Kauf enthält der Chip einen Teil der Firmware im Flash. Er kann vom Anwender nicht verändert werden. Im zweiten, variablen Flash-Bereich steht die Safety-Applikation, die der Anwender programmiert.

5.5 Erfolgt eine statische oder eine dynamische Speicherzuordnung für Daten und Programme? Wo ist dies dokumentiert?

Der Programmspeicher ist statisch zugeordnet.

5.6 Sind weitere "intelligente" Bausteine wie Buskontroller, LAN-Schnittstellen, ASIC, PLD etc. eingesetzt? Wenn ja, gibt es eine detaillierte Beschreibung dieser Bausteine und ihrer Funktionen?

Nicht relevant, da nur das Bus-Interface bestehend aus einem Mikrokontroller betrachtet wird. Der CSC01 muss applikationsspezifisch in eine Baugruppe integriert werden.

5.7 Wurde in der Hardware eine Trennung für sicherheitstechnisch wichtige und betriebliche Funktionen vorgesehen bzw. realisiert?

Nein.

5.8 Gibt es sicherheitstechnisch wichtige Funktionen, die in vom Mikrokontroller/Mikroprozessor unabhängiger Hardware realisiert wurden?

Nein.

5.9 Erfolgte die Auslegung der Komponente mit Uhrzeit oder Kalender? Wenn ja, was wurde festgelegt um Probleme wie Sommer-/Winterzeit-Umschaltung und kritische Kalenderdaten (z. B. Schaltjahreffekte) zu lösen? Wo ist dies dokumentiert?

Die Verwendung von Uhrzeit- bzw. Kalenderfunktionen ist nicht dokumentiert.

5.10 Wurde die Hardware hinsichtlich zu erwartender Alterungseffekte analysiert und welche Reserven wurden hierfür berücksichtigt?

Hierzu sind in den vorliegenden Unterlagen keine Angaben enthalten.

6 Konstruktive Maßnahmen zur Fehlervermeidung bei der Softwareentwicklung

6.1.1 Wie ist die Software der Komponente aufgebaut?

Die Software ist modulatorientiert aufgebaut.

6.1.2 Wurden spezielle Tools zur Versionsverwaltung eingesetzt? Wenn ja, welche?

Die Verwaltung und Kontrolle während des Software-Sicherheitszyklusses erfolgt mit einem Softwareverwaltungsprogramm. Es wird WinCVS eingesetzt, das es ermöglicht, Änderungen an der Software zu verwalten.

6.1.3 Ist der Sourcecode gut strukturiert, lesbar und dokumentiert?

Der Source-Code lag nicht vor.

6.1.4 Wurden bei der Erstellung der Software spezielle Programmierrichtlinien berücksichtigt? Wenn ja, welche Festlegungen finden sich dort und wo sind diese dokumentiert?

Hierzu sind in den vorliegenden Unterlagen keine Angaben enthalten.

6.2.1 Wie ist der Prozess zur Erzeugung des Maschinencodes gestaltet? Kamen Werkzeuge (Tools) für die automatische Generierung von Sourcecode zum Einsatz? Wenn ja, welche, und wo sind diese detailliert beschrieben?

Die Maschinencodeerzeugung erfolgte nach traditionellem Vorgehen mit Compiler, Assembler, Linker und Locator. Zum Einsatz kommt die Entwicklungsumgebung TASKING Tools for M16C v2.3r1.

6.2.2 Welche Programmiersprachen wurden verwendet?

Die Programmierung des CSC01 erfolgte in C/C++. Die vorgelegte Softwarebeschreibung lässt C als Programmiersprache erkennen. Als Entwicklungsumgebung wird TASKING Tools for M16C v2.3r1 der Firma Altium eingesetzt.

6.2.3 Ist der Compiler (Übersetzer) durchgehend getestet und bewährt? Sind evtl. Einschränkungen bekannt? Wurden Compiler-Funktionen zur Optimierung des Codes benutzt? Werden neben den Standard-Bibliotheken noch weitere Bibliotheken benutzt?

Als Compiler wird der Altium C/C++ Compiler, Assembler, Linker und Locator eingesetzt. Der verwendete Compiler ist laut Hersteller bewährt und vielfach in der Entwicklung eingesetzt. Einschränkungen sind nicht bekannt. Die Optimierung des Compilers ist auszuschalten bzw. auf die kleinste Optimierungsstufe einzustellen. Sollte es aus bestimmten Gründen während der Entwicklung dazu kommen, dass die Optimierung verändert werden muss, dann ist dies ausführlich zu begründen und die Auswirkungen auf die Software sind detailliert zu prüfen.

6.2.4 Ist dynamisches Binden zugelassen?

Die Software des CANopen Safety Chip besteht aus zwei grundlegenden Teilen, der permanenten Firmware und der variablen Safety Applikation. Da beide Softwareteile getrennt entwickelt werden, können sie nicht vom Linker der Entwicklungsumgebung miteinander verbunden werden. Es sind Schnittstellen zum wechselseitigen Aufruf notwendig. Eine Sprungtabelle für den Funktionsaufruf und ein Datenspeicher zur Parameterübergabe definieren die Schnittstelle. Der Datenzugriff erfolgt auf festen und beiden Softwareteilen bekannten Adressen.

6.3.1 Wie erfolgte die Modularisierung der Software und wie sind die systeminternen Schnittstellen definiert?

Welche Softwaremodule bzw. Komponenten gibt es?

Wie ist die Softwarestruktur aufgebaut?

Gibt es eine detaillierte Beschreibung der Softwarestruktur?

Gibt es eine detaillierte Beschreibung der Module

(Funktionsbeschreibung, Ein-/Ausgabewerte, etc)?

Die Firmware setzt sich aus mehreren Modulen zusammen. Die einzelnen Module übernehmen unterschiedliche Aufgaben innerhalb der gesamten Applikation. Über die Return-Werte der Funktionen werden der CSC Main Funktion Fehlerzustände mitgeteilt.

Hinsichtlich der Funktionsklassen lehnen sich die sicherheitsrelevanten Module an die Funktionsklassen des Standard CANopen-Stacks an. Diese Klassen sind:

- Initialisierung
- Prozessverarbeitung
- Funktion zur Reaktion auf Ereignisse
- Callback-Funktionen zur Konfiguration von Objekteinträgen
- static-Funktionen

Eine detaillierte Beschreibung der Softwarestruktur und der Module befindet sich in dem Dokument "Softwaredesign". Die Struktur der Programmmodule wird in Flussdiagrammen dargestellt.

6.3.2 Erfolgte eine Modularisierung der Software in überschaubare Einheiten?

Die Software des CSC01 besteht aus zwei grundlegenden Teilen, der permanenten Firmware und der anwenderspezifischen Safety-Applikation. Die permanente Firmware enthält den CANopen-Safety-Protokoll-Stack mit allen sicherheitsrelevanten Kommunikationsfunktionen, sowie Diagnosefunktionen für RAM, Register, Stack und Flash. Sie setzt sich aus mehreren Modulen zusammen. Im zweiten Flash-Bereich steht die Safety-Applikation, die von den Anwendern noch zu programmieren ist.

6.3.3 Wurden Maßnahmen zur eindeutigen Identifikation von Softwareeinheiten getroffen? Wenn ja, wo sind diese dokumentiert?

Zur eindeutigen Identifikation der Softwareeinheiten wird WinCVS (Concurrent Versions System) verwendet. Dieses Programm stellt eine Versionskontrolle und ein Änderungsmanagement für Programmcode zur Verfügung. Die Verwendung von WinCVS stellt eine Kontrolle und Dokumentation der Konfiguration und Änderung sicher.

6.3.4 Gibt es eine eindeutige Zuordnung von Modulen zu den in der Anforderungsspezifikation definierten Funktionen?

Hierzu sind in den vorliegenden Unterlagen keine Angaben enthalten.

6.4 Welche Taskstruktur und Übergangsbedingungen für die Taskwechsel gibt es?

Gibt es eine Taskbeschreibung?

Wie erfolgt die Synchronisation, Zuteilung des Prozessors?

Wo ist dies dokumentiert?

Es existiert keine Task-Struktur.

Die CSC-Mainfunktion ruft das Applikationsprogramm als Funktion auf.

6.5 Wie sind bei mehreren Betriebsarten die Übergangsbedingungen für einen Betriebsartenwechsel definiert? Wo sind diese dokumentiert?

Für den CSC01 existiert nur eine Betriebsart.

6.6 Ist eine Trennung von Betriebs- und Sicherheitsfunktionen in der Software vorgesehen?

Wenn ja, wie erfolgt diese Trennung?

Der CSC01 ist ausschließlich für Sicherheitsfunktionen vorgesehen.

6.7 Wie wird der Kontrollfluss gesteuert?

Der Kontrollfluss der CSC-Main Funktion ist linear aufgebaut und wird zyklisch durchlaufen.

6.8 Welche zeitlichen Randbedingungen wurden festgelegt? Wo sind diese beschrieben?

Aufgrund der Forderung, dass die Restfehlerrate durch das Bussystem auf 1% für SIL3 begrenzt sein soll, können maximal 44 Nachrichten pro Sekunde übertragen werden, was einer Refreshzeit von 23 ms entspricht. Dieses Ergebnis gilt unter der Annahme der maximalen Anzahl von Teilnehmern (64) im Netzwerk und dass alle Teilnehmer mit dieser minimalen Refreshzeit übertragen.

6.9.1 Kann nachgewiesen werden, dass das resultierende Verhalten in vorhersagbarer Weise allein von den sicherheitstechnisch wichtigen Funktionen der Komponente bestimmt wird (deterministisches Verhalten)?

Es sind keine nicht sicherheitstechnisch wichtigen Funktionen vorhanden.

6.9.2 Ist die Unabhängigkeit vom verfahrenstechnischen Anlagenprozess bzw. der zugehörigen Signaltrajektorien für:

- Programmablauf
- Interruptbehandlung
- Arbeitsauslastung der Prozessoren
- Kommunikationsbelastung

sichergestellt?

Aufgrund des zyklischen Austausches von Telegrammen ist der Programmablauf unabhängig vom Prozess.

6.9.3 Erfolgt eine strikt zyklische Bearbeitung aller sicherheitskritischen Funktionen der Komponente?

Die feste Programmzykluszeit ist konfigurierbar in 1 ms Schritten bei einer minimal möglichen Zykluszeit von 20 ms.

6.9.4 Ist die mögliche Variationsbreite in der Programmlaufzeit gering und sind die beeinflussenden Faktoren beschrieben?

Die Programmlaufzeit richtet sich nach der Zykluszeit und ist immer konstant.

**6.10.1 Wird ein Betriebssystem verwendet? Wenn ja, welches?
Garantiert der Hersteller ein definiertes Zeitverhalten (Echtzeitbetriebssystem)?
Verfügt das Betriebssystem über erweiterte Sicherheitsfunktionen?**

Gemäß den Unterlagen wird kein Betriebssystem eingesetzt.

**6.10.2 Sind im Betriebssystem oder der Anwendersoftware Überwachungsmechanismen für den Zugriff auf Speicherbereiche implementiert?
Wenn ja, wo sind diese beschrieben?**

Gemäß den Unterlagen wird kein Betriebssystem eingesetzt.

6.11 Welche Festlegungen zum Interrupthandling gibt es (Prioritäten etc.)? Wo sind diese dokumentiert?

Die Interruptquellen werden nach Hardware- und Softwareinterrupts unterteilt. Die Hardwareinterrupts werden in Spezialinterrupts und periphere I/O-Interrupts unterteilt. Der Mikrocontroller unterscheidet zwei Interruptvektortabellen, eine Feste und eine Variable. Der festen Interruptvektortabelle sind die Spezialinterrupts zugeordnet. Die Softwareinterrupts und die peripheren I/O-Interrupts werden über eine variable Interruptvektortabelle in der CSC Main Funktion verwaltet. Alle Interruptquellen, die nicht von der CSC Main Funktion verwendet werden, kann die Safety Applikation nutzen. Der Einsprung in nicht verwendete Interrupts führt zum sicheren Zustand.

Die Interruptfestlegungen werden in Kapitel 3.11 der Dokumentation "Technische Dokumentation und Nutzerhandbuch" Seite 62ff behandelt. Ebenfalls dokumentiert sind die Prioritäten der Interrupts.

6.12 Wurde vorgefertigte Software eingesetzt?, Wenn ja, wie wurde deren Zuverlässigkeit nachgewiesen?

Es wurde keine vorgefertigte Software eingesetzt.

7 Maßnahmen zur Fehlererkennung und Fehlerbeherrschung

7.1 Welche (Selbst-) Überwachungsfunktionen für die ordnungsgemäße Funktion der rechnergestützten Komponente sind implementiert? Wo sind diese detailliert beschrieben?

Die Maßnahmen zur Fehlererkennung und -beherrschung wurden im Vorfeld der Zertifizierung nach IEC 61508 in einem Design Review vom TÜV Rheinland verifiziert (u. a. CPU, OP-Code, System Stack, Register, interne Peripherie). Eine Diagnose des RAM erfolgt mit einem Galpat-Test, der sich alle 68 min wiederholt. Sicherheitsrelevante Daten werden redundant im RAM abgelegt.

Eine detaillierte Beschreibung der Überwachungsfunktionen befindet sich in dem Dokument "Softwaredesign".

7.2.1 Werden die Speicherbereiche, die den Programmcode oder unveränderliche Daten enthalten, überwacht? Wenn ja, auf welche Weise und wo ist dies dokumentiert?

Der flüchtige Speicher (RAM) wird mit einem Galpat-Test alle 68 min überprüft. Der nicht-flüchtige Speicher (Flash) des CRC01 wird zyklisch mit einer CRC-Summe geprüft. Die CRC-Summe muss außerhalb des Mikrocontrollers (z. B. von einem PC) berechnet werden und wird im Flash abgelegt. Der Test vergleicht den intern berechneten Wert mit dem im Flash abgelegten. Bei Änderungen der Software muss die abgelegte CRC-Summe aktualisiert werden.

Dokumentiert ist die Diagnose des Speichers u. a. in der "CANopen Safety Chip Kurzbeschreibung".

7.2.2 Gibt es Speicherzugriffsüberwachungen (z. B. hinsichtlich Feldindizes)?

Hierzu sind in den vorliegenden Unterlagen keine Angaben enthalten.

7.3.1 Erfolgt eine Prüfung der Eingangs- und Ausgangsdaten auf Einhaltung des Wertebereichs?

Hierzu sind in den vorliegenden Unterlagen keine Angaben enthalten.

7.3.2 Erfolgt eine Prüfung der Zwischenwerte auf zulässige Wertebereiche?

Hierzu sind in den vorliegenden Unterlagen keine Angaben enthalten.

7.3.3 Gibt es eine Überwachung hinsichtlich der Einhaltung der Wertebereiche der Modulein- und -ausgabewerte?

Hierzu sind in den vorliegenden Unterlagen keine Angaben enthalten.

7.4 Gibt es Überwachungsfunktionen für komponenteninterne Busfunktionen? Wenn ja, wo sind diese dokumentiert?

Die typgeprüfte Komponente, die nur aus einem Mikrokontroller besteht, besitzt keine Busfunktionen.

7.5 Erfolgt eine Überwachung des Datenverkehrs über die Datenschnittstellen? Wenn ja, wo ist dies dokumentiert?

Fehler auf dem CAN-Bus bei der Übertragung sicherheitsrelevanter Nachrichten werden entsprechend IEC 61508 durch folgende Maßnahmen erkannt:

- Datenverfälschung: Erkennung durch bitweise inverse redundante Telegramme (Ein Telegramm wird zeitversetzt über ein CAN-Businterface im Original und über das zweite in invertierter Logik gesendet.)
- Verlust, Verzögerung: Erkennung durch Zeitüberwachung
- Falsche Reihenfolge/Abfolge/Wiederholung: Erkennung durch Nummerierung der Telegramme
- Wiederholung und Einfügung: Erkennung durch logische Programmüberwachung und die Verwendung von zwei CAN-Controllern
- Unterscheidung von sicherheitsrelevanten und nicht-sicherheitsrelevanten Nachrichten durch einen speziellen Identifier, um eine Auswertung von nicht-sicherheitsrelevanten Nachrichten durch sicherheitsrelevante Teilnehmer aufgrund von Fehladressierungen zu verhindern

Die Überwachungsfunktionen sind im Prüfbericht vom TÜV Rheinland dokumentiert.

7.6.1 Welches Fehlerverhalten hat die Komponente?

Wird ein Diagnosefehler oder ein Fehler im CAN-Treiber festgestellt, so verweilt die Main-Funktion in einer Endlosschleife im sicheren Zustand STOPP. In diesem Zustand wird der Watchdog nicht mehr getriggert und die CAN-Kommunikation wird abgeschaltet. Alle Interrupts werden gesperrt. Neben diesen Mechanismen des CSC01 obliegt es dem Applikationshersteller, einen Watchdog mit externer Zeitbasis und zweitem Abschaltweg zu implementieren.

Werden Telegrammfehler festgestellt, erfolgen innerhalb des zeitlich möglichen Rahmens Wiederholungen.

7.6.2 Wie verhält sich die Komponente bei Störungen in der Stromversorgung?

Der CSC01 benötigt eine 5V Spannungsversorgung. In Abhängigkeit der gegebenen Sicherheitsanforderungen ist eine Überwachungsschaltung auf Über- oder Unterspannung notwendig. Beim Ansprechen dieser Schaltung müssen die sicherheitsgerichteten Ausgänge des CSC01 in den sicheren Zustand (vgl. 2.11) gebracht werden. Diese Funktion, sowie eventuelle periodische Tests der Überwachungsschaltung, müssen Bestandteil der Applikationssoftware sein.

**7.7 Gibt es eine Protokollierung bei Störungen oder Fehlern im Gerät?
Wenn ja, wie erfolgt diese Protokollierung?**

Es erfolgt keine Protokollierung. Bei fehlerhaftem Verhalten wird der sichere Zustand angefahren, d. h. die Buskommunikation wird eingestellt und die Ausgänge werden über eine Sicherheitsschalteneinrichtung abgeschaltet (vgl. 2.11).

8 Schnittstellen

8.1 Welche systeminternen und externen Schnittstellen hat das Gerät?

Die Komponente besitzt zwei interne CAN Controller, die redundant genutzt werden. Die Anschaltung an die Bus-Leitungen erfolgt über einen CAN-Transceiver und eine entsprechende EMV-Beschaltung.

Die Schnittstelle zur Applikation erfolgt über Funktionsaufrufe der Applikationssoftware im CSC Main Programm und Datenaustausch zwischen diesen beiden Programmteilen.

8.2 Wie ist das implementierte Verhaltensmuster des Geräts / Systems an den Datenschnittstellen?

Nicht relevant, da nur das Bus-Interface bestehend aus einem Mikrokontroller betrachtet wird. Der CSC01 muss applikationsspezifisch in eine Baugruppe integriert werden.

8.3 Was kann über die vorhandenen Schnittstellen an den Einrichtungen verändert werden (Parameter, Firmware)?

Über die Bedienerschnittstelle kann das kompilierte Applikationsprogramm in den Flash-Bereich des CSC01 geladen werden. Die Safety-Applikationen sind permanent als Firmware gespeichert und können nicht verändert werden.

8.4.1 Welche Mechanismen zum Schutz des Programmcodes und der Parameterdaten gegen unbeabsichtigte oder unbefugte Änderungen im Betrieb wurden implementiert?

Die Firmware ist nicht löschar im ROM-Speicher abgelegt. Der Schutz der Anwendersoftware muss vom Applikationshersteller vorgesehen werden (z. B. Einbau des Chips in ein geschlossenes Gehäuse).

Die Programmierung des Flash-Speicher des Mitsubishi M306NAFGTFP erfolgt im Programmiermodus. Dieser Modus wird über den Bootjumper und Reset aktiviert. Erst dann kann mit entsprechenden Programmierertools der Microcontroller über die serielle Schnittstelle programmiert werden. Während der Programmierung muss der Bootjumper geschlossen bleiben.

8.4.2 Welches Verhalten zeigt die Komponente während der Parametrierung oder des Prüfens bzw. der Online-Diagnose?

Es ist keine Parametrierung, Prüfung oder Diagnose im Betrieb vorgesehen.

8.4.3 Muss die Komponente nach der Parametrierung oder Prüfung von Hand aus dem Parametrier- oder Prüfmodus wieder in den Betriebsmodus umgeschaltet werden oder erfolgt dies automatisch?

Es ist keine Parametrierung, Prüfung oder Diagnose im Betrieb vorgesehen.

8.6 Verfügt der eingesetzte Mikrokontroller über eine Bootstraploader-Funktionalität?

Wenn ja, wann und zu welchem Zweck wird er eingesetzt und in welchem Modus wird er betrieben und wo ist dies beschrieben?

Eine Bootstraploader-Funktionalität wird nicht bereitgestellt.

8.7 Wurde die Mensch-Maschine-Schnittstelle nach bestimmten Regeln aufgebaut?

Es ist keine Mensch-Maschine-Schnittstelle vorhanden.

8.8 Wurden für die Analogeingänge der Komponente geeignete Filter in der Hard- oder Software vorgesehen?

Für Interface-Baugruppen nicht relevant.

8.9 Wurden Maßnahmen für die zeitrichtige Behandlung von Binärsignalen getroffen?

Für Interface-Baugruppen nicht relevant.

8.10 Welche Maßnahmen wurden für die binären Eingänge getroffen um technologisch bedingte unerwünschte Signalwechsel (wie Kontaktprellen) zu behandeln?

Für Interface-Baugruppen nicht relevant.

9 Spezielle Fragen zu Interface-Baugruppen

9.1.1 Welche Netztopologien sind möglich?

Die Busteilnehmer werden linienförmig an ein gemeinsames zweiadriges Buskabel angeschlossen.

9.1.2 Sind redundante Busstrukturen möglich?

Je nach Applikation, in der das Businterface eingesetzt wird, prinzipiell möglich.

9.1.3 Ist ein Mischbetrieb mit nicht-sicherheitsgerichteten Nachrichten auf einer Kommunikationsverbindung möglich?

Wie wird die gegenseitige Beeinflussung sicherheitsrelevanter und nicht sicherheitsrelevanter Nachrichten verhindert?

Ein Mischbetrieb ist möglich. Die Trennung der zwei Bereiche erfolgt durch unterschiedliche CAN-Identifizier.

9.2.1 Ist eine Übertragung über Lichtwellenleiter (LWL) möglich?

Der zertifizierte CANopen Safety Chip ist nur für Kupfer-Verbindungen ausgelegt. Da die Telegramme sich an die CANopen-Spezifikation halten, können passive Standard-Komponenten für CANopen, wie z. B. Umsetzer von kupferleitungsbasierter Übertragung zu LWL, prinzipiell verwendet werden.

9.2.2 Können konventionelle Netzwerkkomponenten für den Aufbau der Netztopologie verwendet werden?

Aktive Standard-Komponenten, wie z. B. Switches mit Routing-Eigenschaften, dürfen für die sicherheitsgerichtete Kommunikation nicht verwendet werden.

9.2.3 Welche Verbreitung hat die Komponente in der Industrie?

Fertige Komponenten mit dem CSC01 als Businterface sind noch selten, da die Entwicklung und Typprüfung erst im Juli 2004 abgeschlossen wurde.

9.3.1 Ist die direkte Kommunikation von peripheren Busteilnehmern ohne Sicherheitszentrale möglich?

Der Buszugriff mittels Arbitrierung erlaubt direkte Adressierung und Broadcast-Nachrichten und damit die direkte Kommunikation von peripheren Busteilnehmern ohne eine Sicherheitszentrale.

9.3.2 Welches Konzept liegt dem sicherheitsgerichteten Bussystem zugrunde?

Es erfolgte die Ergänzung von im Protokoll von CANopen bestehenden Sicherungsmaßnahmen durch zusätzliche Hardwaremaßnahmen (redundante CAN-Controller mit Kreuzvergleich).

9.3.3 Welches Buszugriffsverfahren wird verwendet?

Das Buszugriffsverfahren ist zufällig (stochastisch) mit CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance).

Durch zusätzliche im CANopen Safety Protokoll implementierte Maßnahmen, wie z. B. zyklische Datenübertragung und Timerüberwachung, werden die Nachteile eines stochastischen Buszugriffsverfahrens (z. B. keine Deterministik oder Verzögerungen bei der Übertragung von Telegrammen) kompensiert.

9.3.4 Können die Nachrichten mit Prioritäten versehen werden?

Nachrichten können über ihren CAN-Identifizier mit Prioritäten versehen werden. Nachrichten mit höherprioritärer ID werden beim Arbitrierungsprozess bevorteilt.

9.3.5 Wie ist das Verhalten des Bussystems bezüglich der Reaktionszeit?

Ein gleichzeitiger Zugriff von Teilnehmern auf den Bus wird systembedingt nicht verhindert. Die Auswahl der sendeberechtigten Nachricht erfolgt durch Arbitrierung. Diese Technik ermöglicht kurze Reaktionszeiten. Probleme hinsichtlich der Deterministik oder Verzögerungen bei der Übertragung von Telegrammen werden durch zusätzliche im CANopen Safety Protokoll implementierte Maßnahmen kompensiert.

9.3.6 Ist die der Baugruppe zugrunde liegende Protokollspezifikation herstellereinspezifisch oder ein offengelegtes Protokoll?

CANopen ist als offenes System im Auftrag der Nutzerorganisation "CAN in Automation" entwickelt worden. In der Automobilindustrie ist es weit verbreitet und wird zunehmend auch in anderen Industriebereichen eingesetzt.

9.3.7 Wie groß ist die Hamming-Distanz der Datenübertragung auf dem Bussystem?

Die Hamming-Distanz ist 6, d. h. bis zu 5 Bitfehler können erkannt und korrigiert werden.

9.4.1 Werden die typischen Fehler für Buskommunikation (Verlust, Wiederholung, Einfügung, falsche Abfolge, Verzögerung und Nachrichtenverfälschung) beherrscht? Welche Maßnahmen werden bei Fehlererkennung ergriffen?

Die Fehlertypen werden beherrscht durch:

- Zeiterwartung im sicherheitsgerichteten Empfänger.
- Prüfung bezüglich der Reihenfolge und der Priorität der CAN-Identifizier.
- Zeitversetztes Senden der redundanten CAN-Telegramme mit Kreuzvergleich beim Empfänger.

Wird ein Kommunikationsfehler oder ein Fehler im CAN-Treiber festgestellt, so verweilt die Main-Funktion in einer Endlosschleife im sicheren Zustand STOPP. In diesem Zustand wird der Watchdog nicht mehr getriggert und die CAN-Kommunikation wird abgeschaltet. Alle Interrupts werden gesperrt. Da in diesem Zustand der Watchdog nicht mehr bedient wird, werden die Ausgänge eines Aktors über den zweiten Abschaltweg in den sicheren Zustand gesetzt.

9.4.2 Wie wirkt sich der Ausfall einzelner Busteilnehmer auf das Netzwerk aus?

Da alle Busteilnehmer gleichzeitig auf den Bus zugreifen und somit keine Abhängigkeiten (z. B. Weitergabe eines Tokens) zwischen den Busteilnehmern bestehen, hat der Ausfall einzelner Busteilnehmer keine Auswirkung auf das Netzwerk.

9.4.3 Wird ein Watchdog verwendet?

Der Chip CSC01 besitzt keinen eigenen Watchdog. Der Typprüfbericht fordert allerdings, dass wenn der CSC01 in einer Aktoranwendung eingesetzt wird, ein externer Watchdog mit eigener Zeitbasis und zweitem Abschaltpfad aufgebaut werden muss, um den Programmablauf des CSC01 zu überwachen.



Anhang III: Anforderungen an Interfaces

Anhang III.1 Aufrechterhaltung des Defence-in-Depth-Konzeptes (6 Seiten)

Anforderungen an Interfaces: Aufrechterhaltung des Defence-in-Depth-Konzeptes

Dokumentenstelle		Kat. A	Kat. B	ID
Anforderung				
Stichwort	a) Allgemeine/Übergeordnete Anforderung			
RSK-LL	7.3.5 (8)	☒	☒	467
Verbindungen der Sicherheitsleittechnik der Kategorien 1 und 2 zu anderen Datenverarbeitungs- oder Datenübertragungseinrichtungen sind grundsätzlich zu vermeiden. Sofern sie unvermeidbar sind, sind sie so auszuführen, dass darüber keine Einwirkungen auf die Sicherheitsleittechnik möglich sind.				
KTA 3501	4.7 (2)	☒	☒	177
Das Reaktorschutzsystem muss von den Betriebssystemen so unabhängig sein, dass beim bestimmungsgemäßen Betrieb und bei versagenauslösenden Ereignissen in den Betriebssystemen die Funktion des Reaktorschutzsystems erhalten bleibt.				
IAEA NS-R-1	6.86	☒	☐	342
Störungen zwischen dem Schutzsystem und dem Steuer- und Regelsystem müssen durch die Vermeidung von Verbindungen oder durch geeignete funktionale Trennung verhindert werden. Wenn Signale gemeinsam von beiden, Schutzsystem und ein Steuerungs- und Regelsystem, genutzt werden, muss eine geeignete Trennung (wie durch eine angemessene Entkopplung) sichergestellt werden und es muss nachgewiesen werden, dass alle Sicherheitsanforderungen an das Schutzsystem eingehalten werden.				
Stichwort	c) Anforderung an die Auslegung			
RSK-LL	7.3.5 (4)	☒	☒	463
Die Sicherheitsleittechnik muss von der Betriebsleittechnik unabhängig sein, so dass bei versagenauslösenden Ereignissen in der Betriebsleittechnik die Funktion der Sicherheitsleittechnik erhalten bleibt.				
RSK-LL	7.3.5 (6)	☒	☒	465
Innerhalb der Sicherheitsleittechnik müssen die Einrichtungen der verschiedenen Kategorien unabhängig sein, so dass bei versagenauslösenden Ereignissen in den Einrichtungen der sicherheitstechnisch niederwertigeren Kategorie die Funktionen der sicherheitstechnisch höherwertigeren Kategorie erhalten bleiben.				

Stichwort

c) Anforderung an die Auslegung

KTA 3501	7 (2)	☐	☒	279
----------	-------	--------------------------	-------------------------------------	-----

Die Zustandsbegrenzungen sind redundant aufzubauen und rückwirkungsfrei gegeneinander und gegen die Betriebssysteme zu entkoppeln.

VDI/VDE 3527	5.2.3	☒	☐	1208
--------------	-------	-------------------------------------	--------------------------	------

Im Falle der Kommunikation zwischen Leitsystemen mit unterschiedlicher Sicherheits-Kategorisierung erfolgt die Übertragung von Prozessdaten generell nur von Systemen der höheren zur niedrigeren Kategorie.

VDI/VDE 3527	5.2.3	☒	☐	1207
--------------	-------	-------------------------------------	--------------------------	------

Keine direkte Kommunikation zwischen Leitsystemen, deren Unabhängigkeit gewährleistet sein soll.

VDI/VDE 3527	3.4	☒	☐	1194
--------------	-----	-------------------------------------	--------------------------	------

Die konsequente Realisierung des Defence-in-Depth Prinzips und eines hohen Redundanzgrades bei der Auslegung der Leittechnik führt nicht zwangsläufig zur gewünschten Fehlertoleranz, wenn nicht wirksame Maßnahmen zur Verhinderung einer Fehlerausbreitung vorgesehen werden. Hierbei sind nicht nur Fehlerausbreitungsmechanismen zu betrachten, durch die mehrere, redundante Teilsysteme oder Systeme verschiedener leittechnischer Barrieren gleichzeitig beeinflusst werden können, sondern auch solche Fehlerausbreitungsmechanismen, bei denen - vergleichbar dem Dominoeffekt - erst durch den ersten Fehler selbst die energetischen, datentechnischen oder funktionalen Voraussetzungen für Folgefehler geschaffen werden. Gegen letztgenannte Fehler auszulegen bedarf bei komplexen Systemen umfangreicher Analysen zu Fehlereffekten und Fehlerauswirkungen. Zur Sicherstellung der Unabhängigkeit von leittechnischen Teilsystemen im Sinne dieser Richtlinie sind daher unterschiedliche Arten von Sperren zur Fehlerfortpflanzung zu realisieren, um die verschiedenen Barrieren und Redundanten vor einem common-cause-bedingten Versagen zu bewahren und damit die Einhaltung der übergeordneten Schutzziele zu gewährleisten. Der Sinn von funktionalen Barrieren ist die Verhinderung von Auswirkungen des Versagens einer leittechnischen Funktion auf andere leittechnische Funktionen, die aus der Sicht der Verfahrenstechnik unabhängig von der ausgefallenen Funktion wirken sollen. Bei der Auslegung ist hierbei insbesondere das Vorsehen von unabhängigen Komponenten oder Teilsystemen und die geeignete Verteilung der leittechnischen Funktionen auf diese zu beachten.

IAEA NS-R-1	5.3	☒	☒	71
-------------	-----	-------------------------------------	-------------------------------------	----

Geeignet ausgelegte Schnittstellen müssen zwischen den Gebäuden, Systemen und Komponenten unterschiedlicher Kategorien vorgesehen werden, damit ein Versagen in einem System einer niedrigeren Kategorie sich nicht in ein System einer höheren Kategorie ausbreiten kann.

IAEA NS-G-1.1	5.13	☒	☒	1283
---------------	------	-------------------------------------	-------------------------------------	------

Die Systemschnittstellen wie auch die Schnittstellen zu einem Anlagennetzwerk sollen so ausgelegt werden, dass sie nicht andere Schutzaktionen, die durch externe Systeme durchgeführt

Anforderung

Stichwort

c) Anforderung an die Auslegung

werden, gefährden. Fehlfunktionen und Versagen von externen Systemen oder Hilfssystemen sollen bewirken, dass das System in einen sicheren Zustand gebracht wird.

IAEA NS-G-1.3	5.59	☒	☒	779
---------------	------	-------------------------------------	-------------------------------------	-----

Datenflüsse von Systemen einer niedrigeren Sicherheitskategorie zu Systemen einer höheren Sicherheitskategorie sollen grundsätzlich, soweit praktisch möglich, vermieden werden. Wenn solche Datenflüsse unentbehrlich sind, sollen Maßnahmen getroffen werden, die sicherstellen, dass die Daten aus den Systemen der niedrigeren Kategorie sicherheitstechnisch wichtige Funktionen nicht gefährden können.

IAEA NS-G-1.3	2.44	☒	☒	661
---------------	------	-------------------------------------	-------------------------------------	-----

Alle Leittechniksysteme und -geräte, die sicherheitstechnisch wichtige Funktionen ausführen, sollen angemessen ausgelegte Schnittstellen mit Systemen oder Geräten anderer Klassen haben, um sicherzustellen, dass jedes Versagen in einem System einer niedrigeren Klasse sich nicht in ein System einer höheren Klasse ausbreitet. Die Einrichtungen, die für die Verhinderung der Ausbreitung eines Versagens vorgesehen werden, sollen so behandelt werden, wie wenn sie der höheren Klasse angehören.

IAEA NS-G-1.3	4.37	☒	☒	686
---------------	------	-------------------------------------	-------------------------------------	-----

Unabhängigkeit soll zur Verhinderung von folgenden Ausbreitungsmöglichkeiten von Ausfällen betrachtet werden:

- zwischen oder innerhalb von Systemkomponenten als Auswirkung von PIEs,
- zwischen oder innerhalb von Systemen der gleichen sicherheitstechnischen Bedeutung und
- von Systemen mit geringerer sicherheitstechnischer Bedeutung zu Systemen mit höherer sicherheitstechnischer Bedeutung.

IAEA NS-G-1.3	4.44	☒	☒	691
---------------	------	-------------------------------------	-------------------------------------	-----

Kein anzunehmendes Versagen auf der Nicht-Sicherheitsseite der Trenneinrichtung soll während oder nach einem PIE, das erfordert, dass die Sicherheitsfunktion ausgeführt wird, irgendeinen Teil des Sicherheitssystems an der Erfüllung der minimalen Leistungsanforderungen hindern.

IAEA NS-G-1.3	5.32	☒	☐	756
---------------	------	-------------------------------------	--------------------------	-----

Mögliche Wechselwirkungen zwischen dem Reaktorschutzsystem und dem Regelungssystem sollen untersucht werden. Wenn Signale von beiden gemeinsam genutzt werden, muss eine angemessene Trennung (wie z. B. eine angemessene Entkopplung) sichergestellt werden.

IEC 60709	4.1	☒	☐	1366
-----------	-----	-------------------------------------	--------------------------	------

Systeme, die Funktionen der Kategorie A ausführen, müssen vor physikalischen Folgewirkungen von Fehlern und üblichen Handlungen geschützt werden, die auftreten innerhalb von

Anforderung

Stichwort

c) Anforderung an die Auslegung

- a) redundanten Teilen jener Systeme und
b) Systemen einer niedrigeren Kategorie.

Die in Betracht gezogenen Fehler müssen sowohl die innerhalb des leittechnischen Systems und seiner Stromversorgung als auch die als Ergebnis von Ereignissen außerhalb des leittechnischen Systems auftretenden Fehler umfassen.

In manchen Fällen kann es notwendig sein, eine physikalische Trennung zwischen unterschiedlichen Systemen, die Funktionen der Kategorie A ausführen, vorzusehen, wenn Unabhängigkeit zwischen diesen Funktionen gefordert wird.

IEC 60709 4.1 ☐ ☒ 1367

Systeme, die Funktionen der Kategorie B ausführen, müssen vor physikalischen Folgewirkungen von Fehlern und üblichen Handlungen geschützt werden, die auftreten innerhalb von

- a) redundanten Teilen jener Systeme und
b) Systemen einer niedrigeren Kategorie.

Die in Betracht gezogenen Fehler müssen die innerhalb des leittechnischen Systems und seiner Stromversorgung auftretenden Fehler umfassen, die als Ergebnis von Ereignissen außerhalb des leittechnischen Systems auftretenden Fehler dürfen unberücksichtigt bleiben. Wenn Funktionen der Kategorie B als Schutz für bestimmte Störfälle vorgesehen sind, müssen die ausführenden Systeme nach den Prinzipien eines Systems für Kategorie-A-Funktionen ausgelegt sein.

IEC 60709 4.1 ☒ ☒ 1369

Wo physikalische Trennung verlangt wird, müssen Vorkehrungen gegen eine Ausfallfortpflanzung in Betracht gezogen werden

- für Ausfälle, die als Folge von anzunehmenden versagenauslösenden Ereignissen (AVE) gleichzeitig Komponenten in Mehrfachsystemen betreffen,
- zwischen Systemen, die Funktionen der gleichen Kategorie ausführen,
- zwischen redundanten Sicherheitsgruppen desselben sicherheitstechnisch wichtigen Systems und
- von Systemen mit Funktionen niedrigerer Kategorie zu Systemen mit Funktionen höherer Kategorie und in einigen speziellen Fällen von Systemen mit Funktionen höherer Kategorie zu Systemen mit Funktionen niedrigerer Kategorie.

Die Arten möglicher versagenauslösender Ereignisse in den folgenden Unterabschnitten müssen in Betracht gezogen werden (z. B. ermittelt, dokumentiert und begründet). Geeignete Vorkehrungen müssen für sicherheitstechnisch wichtige leittechnische Systeme getroffen werden, um mögliche Auswirkungen dieser Ereignisse auf ein annehmbares Maß zu beschränken. Betrachtet werden sollten auch die Auswirkungen der Kombination von Ausfallereignissen.

IEC 60709 5.3 ☒ ☒ 1381

Wenn Signale von Geräten eines Kategorie-A-Systems (N1) zu Systemen mit niedrigerer Kategorie übertragen werden, muss dies über Isolationseinrichtungen geschehen, die dem Kategorie-A-System angehören. Die Isolationseinrichtung muss so ausgelegt sein, dass Ausfälle oder Bedingungen an ihren Ausgängen (die mit den Systemen niedrigerer Kategorie

Anforderung

Stichwort

c) Anforderung an die Auslegung

verbunden sind) eine Sicherheitsaktion des Kategorie-A-Systems oder -Teilsystems, mit der die Isolationseinrichtung verbunden ist, nicht verhindern können. Die vorgesehene elektrische Isolationseinrichtung muss die Anforderungen in 5.3.2 erfüllen.

Für Wartungszwecke müssen zeitweise Verbindungen ohne Isolationseinrichtung mit Kategorie-A-Systemen gestattet werden, vorausgesetzt, die Verbindung besteht zu jedem Zeitpunkt nur mit einem einzigen Strang eines redundanten Systems, die Verbindung wird nach Gebrauch aufgehoben, und das System ist in der Lage, einen durch Ausfall oder Verwendung der Verbindung eingeschleiften Fehler zu beherrschen.

Es muss ein Schutz gegen folgende Ausfälle und Bedingungen sichergestellt sein:

- a) Kurz- und Erdschlüsse;
- b) Unterbrechungen;
- c) Aufschaltung der maximalen Wechsel- oder Gleichspannung, die vernünftigerweise auftreten kann, wobei die verfügbaren Spannungsquellen und Potentiale in den Kategorie-A-Systemen und sonstigen Systemen in Betracht zu ziehen sind;
- d) elektromagnetische und elektrostatische Beeinflussung.

Hinsichtlich der Eigenschaften einer Isolationseinrichtung sind zu berücksichtigen:

- Toleranz und Isolierung gegenüber elektrischen Schwingungen und Spitzen nach IEC 61000-6-5;
- Toleranz und Isolierung gegenüber elektromagnetischer Beeinflussung nach IEC 61000-6-5;
- einfache Barrieren zur elektrischen Isolierung zwischen nahen oder benachbarten Endverbindungen oder Kontaktgruppen an Relais;
- Vorsorge gegen Übertragung außerordentlich hoher oder zerstörender Spannungen.

In diesem Zusammenhang sollte eine Untersuchung über die maximale Spannung, die unter normalen und fehlerhaften Bedingungen zu erwarten ist, durchgeführt werden, und die möglichen Auswirkungen auf das sicherheitstechnisch wichtige Gerät sollten untersucht werden, wenn diese Spannung auf die Endverbindungen der Isolationseinrichtung auf der Seite der sicherheitstechnisch weniger wichtigen Einrichtungen aufgeschaltet wird.

Weiter sollten Vorkehrungen getroffen werden, um die Möglichkeit zu minimieren, dass Ausfälle in nicht sicherheitsrelevanten Systemen spontane ungewollte Aktionen von Funktionen der Kategorie A auslösen.

Werden Anlagengeräte, die von einem Kategorie-A-System angesteuert werden, auch von Signalen eines Systems niedrigerer Kategorie angesteuert, müssen Isolationseinrichtungen vorgesehen sein, die einen Vorrang der vom Kategorie-A-System ausgehenden Steuersignale sicherstellen. Ausfälle im oder normale Aktionen des Systems niedrigerer Kategorie dürfen die Funktionen des Kategorie-A-Systems unter Anlagenbedingungen, die einen Erfolg dieser Funktionen erfordern, nicht überlagern. Die Isolationseinrichtungen zur Sicherstellung des Vorrangs müssen als Teil des Kategorie-A-Systems eingeordnet sein.

Ausfälle und Fehlbetätigungen in Systemen, die nicht entsprechend Kategorie A eingeordnet sind, dürfen keinerlei Rückwirkungen auf das Ansprechverhalten, die Drift, Genauigkeit,

Stichwort

c) Anforderung an die Auslegung

Rauschempfindlichkeit oder andere Eigenschaften des Kategorie-A-Systems haben, die seine Fähigkeit beeinträchtigen könnten, die geforderten Sicherheitsfunktionen auszuführen.

Wenn Signale von Kategorie-B-Systemen oder Kategorie-C-Systemen zur Verwendung in Systemen niedrigerer Kategorie ausgekoppelt werden, mögen Isolationseinrichtungen nicht gefordert sein; guter Ingenieurpraxis folgend sollte jedoch die Ausfallfortpflanzung verhindert werden. In Fällen, in denen Kategorie-B-Funktionen ausführende Systeme infolge der ausgeführten Funktionen Aspekte von Kategorie-A-Systemen zu berücksichtigen haben, muss eine Isolation vorgesehen werden.

Glasfaserkabel stellen ein sehr wirksames Mittel zur Erzielung elektrischer Isolation dar und sollten, wenn immer möglich, verwendet werden.

IEC 60987	5.3	✓	✓		1396
-----------	-----	---	---	--	------

Keinem System mit geringerer sicherheitstechnischer Bedeutung darf erlaubt werden, die Leistungsfähigkeit eines Systems mit höherer sicherheitstechnischer Relevanz zu beeinflussen. Es muss insbesondere nachgewiesen werden, dass kein Hardware- und kein Softwareversagen des Systems mit geringerer sicherheitstechnischer Bedeutung z. B. die Daten des Systems mit höherer Bedeutung zerstören oder seine Zykluszeit erhöhen kann.

Die Auslegung soll mit den anderen auf der Anlage eingesetzten Systemen zusammenpassen. Das System soll auch gegen Zerstörung und Fehlfunktion als Ergebnis eines Versagens oder aufgrund von Eigenschaften des Systems, mit dem es eine Schnittstelle hat, geschützt werden.

IEC 61226	7.2.1	✓	✓		1398
-----------	-------	---	---	--	------

Zwischen den Funktionen unterschiedlicher Kategorien muss eine hinreichende Trennung erfolgen.

IEC61513	5.3.1.3	✓	✓		1078
----------	---------	---	---	--	------

Die Architektur und die Technologie der Kommunikationsverbindungen müssen sicherstellen, dass die Unabhängigkeitsanforderungen zwischen Systemen erfüllt sind. Zusätzlich zu physikalischer Trennung und elektrischer Isolation sollten in der Auslegung Vorkehrungen getroffen sein, die sicherstellen, dass Probleme der Verbindungsleitungen sich nicht auf Verarbeitungsmodule auswirken.

Kommunikationsverbindungen sollten so ausgelegt werden, dass Datenkommunikation und Betrieb einer Funktion höherer Sicherheitskategorie nicht durch die Datenkommunikation eines niedriger klassifizierten Systems beeinträchtigt werden.



**Anhang III.2 Aufrechterhaltung der verfahrenstechnischen Redundanz der
Anlage (3 Seiten)**

Anforderungen an Interfaces:

Aufrechterhaltung der verfahrenstechnischen Redundanz der Anlage

Dokumentenstelle		Kat. A	Kat. B	ID
Anforderung				
Stichwort	a) Allgemeine/Übergeordnete Anforderung			
KTA 3501	4.12 (3)	☒	☒	205
Für voneinander getrennte verfahrenstechnische Systeme des Sicherheitssystems sollen getrennte Funktionsgruppensteuerungen des Reaktorschutzsystems vorgesehen werden. Dies gilt zum Beispiel für die Hochdruck- und Niederdruck- Notkühlsysteme. (gilt auch für Schutzbegrenzungen)				
Stichwort	c) Anforderung an die Auslegung			
KTA 3501	5.5.4 (1)	☒	☐	265
Die Einzelantriebssteuerungen für ein verfahrenstechnisches System müssen strangweise ohne Vermaschung aufgebaut werden.				
KTA 3501	5.5.3 (2)	☒	☐	262
Die Vorrangsteuerungen müssen strangbezogen aufgebaut werden. Signalverbindungen zwischen verschiedenen Strängen sind nach der Vorrangbildung nicht zulässig.				
KTA 3501	4.9 (2)	☒	☒	189
Das Reaktorschutzsystem ist so aufzubauen, dass die in den aktiven Sicherheitseinrichtungen durch Aufteilung in sicherheitstechnisch wichtige Teilsysteme vorgegebene Redundanz gewahrt bleibt. (gilt auch für Schutzbegrenzungen)				
VDI/VDE 3527	5.2.3	☒	☐	1207
Keine direkte Kommunikation zwischen Leitsystemen, deren Unabhängigkeit gewährleistet sein soll.				
VDI/VDE 3527	3.4	☒	☐	1194
Die konsequente Realisierung des Defence-in-Depth Prinzips und eines hohen Redundanzgrades bei der Auslegung der Leittechnik führt nicht zwangsläufig zur gewünschten Fehlertoleranz, wenn nicht wirksame Maßnahmen zur Verhinderung einer Fehlerausbreitung vorgesehen werden. Hierbei sind nicht nur Fehlerausbreitungsmechanismen zu betrachten,				

Stichwort

c) Anforderung an die Auslegung

durch die mehrere, redundante Teilsysteme oder Systeme verschiedener leittechnischer Barrieren gleichzeitig beeinflusst werden können, sondern auch solche Fehlerausbreitungsmechanismen, bei denen - vergleichbar dem Dominoeffekt - erst durch den ersten Fehler selbst die energetischen, datentechnischen oder funktionalen Voraussetzungen für Folgefehler geschaffen werden. Gegen letztgenannte Fehler auszulegen bedarf bei komplexen Systemen umfangreicher Analysen zu Fehlereffekten und Fehlerauswirkungen. Zur Sicherstellung der Unabhängigkeit von leittechnischen Teilsystemen im Sinne dieser Richtlinie sind daher unterschiedliche Arten von Sperren zur Fehlerfortpflanzung zu realisieren, um die verschiedenen Barrieren und Redundanten vor einem common-cause-bedingten Versagen zu bewahren und damit die Einhaltung der übergeordneten Schutzziele zu gewährleisten. Der Sinn von funktionalen Barrieren ist die Verhinderung von Auswirkungen des Versagens einer leittechnischen Funktion auf andere leittechnische Funktionen, die aus der Sicht der Verfahrenstechnik unabhängig von der ausgefallenen Funktion wirken sollen. Bei der Auslegung ist hierbei insbesondere das Vorsehen von unabhängigen Komponenten oder Teilsystemen und die geeignete Verteilung der leittechnischen Funktionen auf diese zu beachten.

IAEA NS-G-1.3	4.41	✓	✓	690
---------------	------	---	---	-----

Eine angemessene Unabhängigkeit soll zwischen diversitären Funktionen bestehen. Die Angemessenheit der bestehenden Unabhängigkeit soll gerechtfertigt werden.

IAEA NS-G-1.3	4.37	✓	✓	686
---------------	------	---	---	-----

Unabhängigkeit soll zur Verhinderung von folgenden Ausbreitungsmöglichkeiten von Ausfällen betrachtet werden:

- zwischen oder innerhalb von Systemkomponenten als Auswirkung von PIEs,
- zwischen oder innerhalb von Systemen der gleichen sicherheitstechnischen Bedeutung und
- von Systemen mit geringerer sicherheitstechnischer Bedeutung zu Systemen mit höherer sicherheitstechnischer Bedeutung.

IEC 60709	4.1	✓	✓	1369
-----------	-----	---	---	------

Wo physikalische Trennung verlangt wird, müssen Vorkehrungen gegen eine Ausfallfortpflanzung in Betracht gezogen werden

- für Ausfälle, die als Folge von anzunehmenden versagensauslösenden Ereignissen (AVE) gleichzeitig Komponenten in Mehrfachsystemen betreffen,
- zwischen Systemen, die Funktionen der gleichen Kategorie ausführen,
- zwischen redundanten Sicherheitsgruppen desselben sicherheitstechnisch wichtigen Systems und
- von Systemen mit Funktionen niedrigerer Kategorie zu Systemen mit Funktionen höherer Kategorie und in einigen speziellen Fällen von Systemen mit Funktionen höherer Kategorie zu Systemen mit Funktionen niedrigerer Kategorie.

Die Arten möglicher versagensauslösender Ereignisse in den folgenden Unterabschnitten müssen in Betracht gezogen werden (z. B. ermittelt, dokumentiert und begründet). Geeignete Vorkehrungen müssen für sicherheitstechnisch wichtige leittechnische Systeme getroffen werden, um mögliche Auswirkungen dieser Ereignisse auf ein annehmbares Maß zu beschränken. Betrachtet werden sollten auch die Auswirkungen der Kombination von Ausfallereignissen.

IEC61513	5.3.1.3	✓	✓	1078
----------	---------	---	---	------

Anforderung

Stichwort

c) Anforderung an die Auslegung

Die Architektur und die Technologie der Kommunikationsverbindungen müssen sicherstellen, dass die Unabhängigkeitsanforderungen zwischen Systemen erfüllt sind. Zusätzlich zu physikalischer Trennung und elektrischer Isolation sollten in der Auslegung Vorkehrungen getroffen sein, die sicherstellen, dass Probleme der Verbindungsleitungen sich nicht auf Verarbeitungsmodule auswirken.

Kommunikationsverbindungen sollten so ausgelegt werden, dass Datenkommunikation und Betrieb einer Funktion höherer Sicherheitskategorie nicht durch die Datenkommunikation eines niedriger klassifizierten Systems beeinträchtigt werden.



Anhang III.3 Systemarchitektur (7 Seiten)

Anforderungen an Interfaces: Systemarchitektur

Dokumentenstelle		Kat. A	Kat. B	ID
Anforderung				
Stichwort	c) Anforderung an die Auslegung			
BMI/BMU SK	Kriterium 6.1:	☒	☐	43
Redundante Teile des RSS sollen grundsätzlich voneinander unabhängige Einrichtungen zur Messwerterfassung und Signalverarbeitung besitzen. Verknüpfungsstellen dürfen die Redundanz und die Auslösesicherheit nicht verschlechtern.				
RSK-LL	7.3.5 (1)	☒	☒	460
Die Sicherheitsleittechnik ist so aufzubauen, dass die in den aktiven Sicherheitseinrichtungen vorgegebene Redundanz gewahrt bleibt.				
RSK-LL	7.2.1 (3)	☒	☐	593
Ein einzelnes versagenauslösendes Ereignis darf die erforderliche Funktion des Sicherheitssystems im Bedarfsfall nicht verhindern.				
RSK-LL	7.3.2 (5)	☒	☐	615
Bei der Auslegung der Sicherheitsleittechnik der Kategorie 1 ist Vorsorge gegen systematische Ausfälle zu treffen				
RSK-LL	7.3.2 (6)	☒	☐	616
Es ist nachzuweisen, dass die Sicherheitsleittechnik der Kategorie 1 ihre Aufgaben auch dann erfüllt, wenn zusätzlich zum Störfall ein Zufallsausfall und ein systematischer Ausfall und Folgeausfälle eintreten. Ein systematischer Ausfall braucht dann nicht angenommen werden, wenn ausreichende Maßnahmen zu seiner Vermeidung nachgewiesen werden. Während eines Instandhaltungsfalls ist auch ein Störfall zu unterstellen. Dabei brauchen innerhalb einer Zeitspanne von 100 h der systematische Ausfall und der Zufallsausfall nicht überlagert werden.				
RSK-LL	7.3.2 (7)	☐	☒	617
Es ist nachzuweisen, dass die Sicherheitsleittechnik der Kategorie 2 ihre Aufgaben auch dann erfüllt, wenn zusätzlich zur Störung ein Zufallsausfall und Folgeausfälle eintreten. Während eines Instandhaltungsfalls ist auch eine Störung zu unterstellen.				

Anforderung

Stichwort

c) Anforderung an die Auslegung

KTA 3501	4.4.1 (2)	☒	☒	157
Es ist nachzuweisen, dass das Reaktorschutzsystem im Zusammenwirken mit aktiven und passiven Sicherheitseinrichtungen zusätzlich zum Störfall a) einen Zufallsausfall b) und einen systematischen Ausfall (soweit er nicht durch eine Analyse ausgeschlossen werden kann)(für Kat. B nicht systemintern) c) und Folgeausfälle beherrscht. (gilt auch für Schutzbegrenzungen)				
KTA 3501	5.5.4 (1)	☒	☐	265
Die Einzelantriebssteuerungen für ein verfahrenstechnisches System müssen strangweise ohne Vermaschung aufgebaut werden.				
KTA 3501	5.5.3 (2)	☒	☐	262
Die Vorrangsteuerungen müssen strangbezogen aufgebaut werden. Signalverbindungen zwischen verschiedenen Strängen sind nach der Vorrangbildung nicht zulässig.				
KTA 3501	7 (2)	☐	☒	279
Die Zustandsbegrenzungen sind redundant aufzubauen und rückwirkungsfrei gegeneinander und gegen die Betriebssysteme zu entkoppeln.				
KTA 3501	4.6 (1)	☒	☒	172
Zur Beherrschung versagenauslösender Ereignisse innerhalb des Reaktorschutzsystems ist ein redundanter Aufbau des Reaktorschutzsystems vorzusehen. (gilt auch für Schutzbegrenzungen)				
KTA 3501	4.2.1	☒	☒	153
Es sind versagenauslösende Ereignisse innerhalb des Reaktorschutzsystems in Betracht zu ziehen, wie zum Beispiel a) Ausfälle durch Kurzschlüsse, Unterbrechungen, Erdschlüsse, Spannungs- und Frequenzänderungen, mechanisches Versagen oder Brände b) mehrere gleichzeitig oder kurzzeitig aufeinander folgende Ausfälle nach a) die eine gemeinsame Ursache (z. B. Fertigungsfehler, Auslegungsfehler, Drift) im System selbst haben, (nicht Kat. B) c) Fehler bei der Bedienung und Wartung des Reaktorschutzsystems durch das Personal. (gilt auch für Schutzbegrenzungen)				

Stichwort

c) Anforderung an die Auslegung

KT A 3501	5.3.2 (2)	☒	☐	231
-----------	-----------	-------------------------------------	--------------------------	-----

Signale zueinander redundanter Einrichtungen dürfen nicht in einem Kabel, einem örtlichen Kabelverteiler und einer Kabeldurchführung geführt werden.

IAEA NS-G-1.1	6.12 - 6.14	☒	☒	1304
---------------	-------------	-------------------------------------	-------------------------------------	------

Rechnersystementwurf

Redundanz in dem Rechnersystem soll im Allgemeinen vorgesehen werden, um die Zuverlässigkeitsanforderungen und die Anforderungen an die Tests während des Betriebs zu erfüllen. Zur Reduzierung von Möglichkeiten eines vernetzten Ausfalls von redundanten Geräten sollen die redundanten Subsysteme elektrisch und physisch getrennt werden. Da das Voting eine gemeinsame Verwendung aller Subsysteme erfordert, soll eine angemessene und ausreichende Zwischenspeicherung verwendet werden, um sicherzustellen, dass die Trennung der redundanten Subsysteme erhalten bleibt. Redundante Subsysteme sollen auch asynchron laufen.

Die Notwendigkeit für die Überbrückung bei der Inbetriebnahme des integrierten Rechnersystems soll berücksichtigt werden, da es Auswirkungen auf das Hardware-Software-Interface haben kann.

IAEA NS-G-1.3	5.58	☒	☒	778
---------------	------	-------------------------------------	-------------------------------------	-----

Wenn die Zuverlässigkeit der Daten und der Datenverbindung von großer Bedeutung ist, soll eine geeignete Kommunikationstechnologie gewählt werden. Eine angemessene Berücksichtigung soll der Verwendung von Redundanz bei der Datenverbindung, dem angemessenen Grad an Vertrauenswürdigkeit der Datenverbindung im Allgemeinen und der Fähigkeit der Sende- und Empfangssysteme, Ausfällen in allen möglichen Betriebsarten zu widerstehen, gewidmet werden. Die Verwendung von Datenkommunikation soll nicht die physische oder funktionale Kanalisierung der Verarbeitung oder der logischen Elemente innerhalb der Systemarchitektur vereiteln.

IAEA NS-G-1.3	4.24	☒	☒	676
---------------	------	-------------------------------------	-------------------------------------	-----

Es soll eine zusätzliche konservative Auslegung vorgesehen werden, wenn der notwendige Nachweis der Systemzuverlässigkeit nicht durchführbar ist, z. B. wenn die Zuverlässigkeit eines mehrfach redundanten Systems durch solche Faktoren wie Common Cause Failures oder Unsicherheiten in der Auslegung begrenzt wird. Spezielle Schwierigkeiten können z. B. bei dem Nachweis der Zuverlässigkeit von rechnerbasierten Systemen auftreten. Diversität ist ein Weg, um eine konservative Auslegung zur Kompensation von Schwierigkeiten bei dem Nachweis des notwendigen Grades von Zuverlässigkeit umzusetzen.

IEC 60709	4.3	☒	☒	1370
-----------	-----	-------------------------------------	-------------------------------------	------

Für jedes sicherheitstechnisch wichtige System müssen dort verursachte versagensauslösende Ereignisse in Betracht gezogen werden. Diese Ereignisse sind üblicherweise durch örtlich beschränkte mechanische und elektrische Auswirkungen charakterisiert, die unterschiedliche funktionale Folgen haben können. Einzelausfälle in zentralen leittechnischen Prozessoreinheiten und an Kommunikationsschnittstellen mit Multiplexern können auch das Potenzial zur Erzeugung von Mehrfachausfällen haben.

Anforderung

Stichwort

c) Anforderung an die Auslegung

Der zufällige Ausfall einer leittechnischen Komponente muss in Betracht gezogen werden, und zwar einschließlich der Energie- oder anderer Hilfsversorgung, die zum Fehlverhalten der Komponente führen kann, einschließlich Kurzschlüssen, Unterbrechung der Kontinuität der Stromkreise, Erdschluss, Spannungs- oder Frequenzänderungen, mechanischem Versagen der Komponenten oder örtlichem Feuer.

Die Folgen der aufgrund eines CCF in zwei oder mehreren Komponenten auftretenden Ausfälle, die sich auf redundante Sicherheitsgruppen auswirken, müssen betrachtet werden. Dabei kann es sich um CCF als Folge von Wartungsfehlern, mechanischer Beschädigung oder elektrischer Interferenz handeln. Umwelteinflüsse, Strahlungsschädigung und andere mögliche gemeinsame physikalische Faktoren müssen berücksichtigt werden.

IEC 60709	4.4.3	✓	✓		1373
-----------	-------	---	---	--	------

Anzunehmende versagenauslösende Ereignisse in Anlagensystemen, Geräten und Strukturen, wie z. B. Feuer, schlagende Rohrleitungen, umherfliegende Teile, mechanische und thermische Auswirkungen, Explosionen oder Leckagen von Wasser, Dampf, Gas, Öl, flüssigem Metall, sowie andere Ereignisse, die potenzielle Verursacher von Beschädigungen sind, müssen in Betracht gezogen werden.

IEC 60709	4.5	✓	✓		1375
-----------	-----	---	---	--	------

Natürliche Ereignisse wie Erdbeben, Überflutung, Stürme, Blitzschlag, Gezeiten oder Flutwellen müssen entsprechend der jeweiligen Lage des Kernkraftwerks in Betracht gezogen werden. Von Menschen außerhalb der Anlage verursachte Ereignisse innerhalb und außerhalb der Anlage, wie z. B. Explosion, Feuer, Flugzeugabsturz, Sabotage müssen in Betracht gezogen werden.

IEC 60709	4.6	✓	✓		1376
-----------	-----	---	---	--	------

Versagenauslösende Ereignisse, die ihre Ursache in besonderen Betriebsbedingungen wie Inbetriebnahme, Modifizierung, Wartung und Reparatur, Auslegungs- und administrativen Kontrollprozeduren haben, müssen in der Auslegungs- und Herstellungsphase berücksichtigt werden, um sie auf ein annehmbares Maß zu reduzieren.

IEC 60709	5.1	✓	✓		1379
-----------	-----	---	---	--	------

Redundantes Gerät leittechnischer Systeme muss zuweilen im Einflussbereich von fest installierten Brandschutzsystemen angeordnet werden. In diesen Fällen müssen das leittechnische System und seine Geräte sowie das Brandschutzsystem so ausgelegt sein, dass der Betrieb des Brandschutzsystems die Unabhängigkeit redundanter Sicherheitsgruppen nicht beeinträchtigt.

Die Leistungsfähigkeit redundanter Sicherheitsgruppen darf durch Feuer und Rauch, die außerhalb eines sicherheitstechnisch wichtigen leittechnischen Systems entstehen, nicht negativ beeinflusst werden. Dieses muss durch räumliche Trennung, Barrieren oder eine Kombination von beiden sichergestellt werden, wobei folgende Anforderungen einzuhalten sind:

a) Der Raum zwischen redundanten Systemen oder Kabeln darf keine Strukturen, Geräte oder Materialien enthalten, die eine Ausbreitung des Feuers unterstützen könnten.

Stichwort

c) Anforderung an die Auslegung

b) Wenn zwischen redundanten Systemen oder Kabeln Barrieren angeordnet sind, müssen diese eine Feuerfestigkeit entsprechend den Brandschutzbestimmungen aufweisen.

IEC 60709	5.2	☒	☒	1380
-----------	-----	-------------------------------------	-------------------------------------	------

Das Gerät leittechnischer Systeme muss so spezifiziert, ausgelegt und installiert sein, dass seine funktionale Fähigkeit während und nach den zu erwartenden Umgebungsbedingungen infolge von Ereignissen nach 4.4 (Versagen auslösende Ereignisse innerhalb der Anlage) und 4.5 (Externe versagen auslösende Ereignisse) sichergestellt ist.

IEC 60709	6.1	☒	☐	1384
-----------	-----	-------------------------------------	--------------------------	------

Redundante Teile von Kategorie-A-Systemen müssen so ausgelegt und installiert sein, dass keines der in Abschnitt 4 angegebenen Einzelereignisse zum Versagen einer Kategorie-A-Funktion führen kann.

IEC 60709	6.1	☐	☒	1385
-----------	-----	--------------------------	-------------------------------------	------

Redundante Teile von Kategorie-B-Systemen müssen so ausgelegt und installiert sein, dass keines der in 4.2 (Auslegungsfehler) und 4.3 (versagen auslösende Ereignisse in leittechnischen Systemen) angegebenen Einzelereignisse zum Versagen einer Kategorie-B-Funktion führen kann. Die Behandlung der in 4.4 (versagen auslösende Ereignisse innerhalb der Anlage) und 4.5 (externe versagen auslösende Ereignisse) angegebenen versagen auslösenden Ereignissen in Bezug auf Kategorie-B-Systeme muss, wie in den allgemeinen Prinzipien von Abschnitt 4 beschrieben, von Fall zu Fall erfolgen.

IEC 61226	7.3.2.2	☐	☒	1041
-----------	---------	--------------------------	-------------------------------------	------

Eine Funktion in dieser Kategorie muss mit redundanten und getrennten Mitteln ausgeführt werden, anderenfalls muss eine Begründung gegeben werden. Eine solche Begründung kann z. B. auf der Fähigkeit eines Systems beruhen, die geforderte Zuverlässigkeit auch ohne die genannten Mittel zu erreichen, auf der Annehmbarkeit der Folgen des Funktionsausfalls oder auf der Verfügbarkeit von genügend Zeit für alternative Maßnahmen bei Funktionsausfall.

IEC 61226	7.3.2.1	☒	☐	1039
-----------	---------	-------------------------------------	--------------------------	------

Ein leittechnisches System, das Funktionen der Kategorie A ausführt, muss redundant sein. Angemessene Trennung muss vorgesehen sein, um sicherzustellen, dass irgendein interner Störfall redundante Stränge des Systems nicht unwirksam machen kann. Ein Einzelausfall darf nicht zum Versagen der vorgesehenen Sicherheitsfunktion führen, auch nicht während präventiver Instandhaltung oder wiederkehrender Prüfung, Inspektion oder Reparatur. Die Anwendung des Einzelausfallkriteriums muss in Übereinstimmung mit 5.34 bis 5.39 von IAEA NS-R-1 sein.

IEC61513	5.3.1.3	☒	☒	1077
----------	---------	-------------------------------------	-------------------------------------	------

Stichwort

c) Anforderung an die Auslegung

Zur Vermeidung von Ausfällen sollte eine angemessene Redundanz der Kommunikationsverbindungen vorgesehen werden.

IEC61513	6.1.1.2.1c,d)	☑	☐	1110
----------	---------------	---	---	------

Die Auslegung von Klasse 1-Systemen muss genügend Redundanz vorsehen, um das Einzelfehlerkriterium (single failure criterion) bei Betrieb und Wartung zu erfüllen.
Die Auslegung von Klasse 1-Systemen muss Unabhängigkeit zwischen den verschiedenen Redundanzen vorsehen.

IEC61513	6.1.2.2	☑	☑	1128
----------	---------	---	---	------

Die Anordnung der Teilsysteme im System muss den Auslegungs-Randbedingungen nach 6.1.1.2 genügen.
Die Anordnung der Teilsysteme im System muss konsistent mit den Anforderungen an die Zuverlässigkeit der Funktionen mit sicherheitstechnischer Bedeutung sein.
Bei der Festlegung der Einbauorte von Teilsystemen in der Anlage und der Übertragungswege zwischen den Teilsystemen sollten die folgenden Faktoren beachtet werden:
- die Auftrennung redundanter Kanäle von Geräten zur Mehrheitsentscheidung kann notwendig sein, um die Auswirkung lokaler Gefährdungen - wie z.B. Feuer - zu reduzieren und, wenn erforderlich, das Einzelfehlerkriterium zu erfüllen (siehe 6.1.1.2.1);
- die Zentralisierung von Funktionen, die Bedeutung für den Zugriffsschutz haben, kann erforderlich werden, um die Anforderung nach Kontrolle nicht-autorisierten Zugangs zu erfüllen.
- die Zentralisierung komplexer Einrichtungen und Geräte kann den Betrieb, die Wiederholungsprüfungen, Wartung und die Kontrolle von Umgebungsbedingungen erleichtern; und
- der Einsatz von Multiplex-Datentransfer kann die Verkabelungskomplexität vermindern.
Wenn Unabhängigkeit gefordert ist, sollte diese erreicht werden durch:
- elektrische Isolation, die durch Lichtleiter, optische Isolatoren oder Kabelschirme erreicht werden kann;
- physikalische Trennung, die durch geeignete Abstände, Barrieren oder eine Kombination aus beiden erreicht werden kann; und
- für rechnerbasierte Systeme Unabhängigkeit der Kommunikation, die durch die Auswahl geeigneter Kommunikationsarchitekturen und Protokolle erreicht werden kann.
Die Systemarchitektur sollte die Wahrscheinlichkeit und die Konsequenzen der Ausbreitung und Nebenwirkungen von Ausfällen minimieren. Die folgenden Techniken können in Betracht gezogen werden:
- interne Isolation, wodurch Ausfälle sich aufgrund des Fehlens von Ausbreitungspfaden und von gemeinsam genutzten Mitteln nicht ausbreiten können;
- Systemüberwachung mit internen (z.B. Selbstüberwachung) oder externen Einrichtungen (z.B. andere Systeme oder Operateure), wodurch die Früherkennung verfälschter Daten und/oder schadhafter Hilfsmittel ermöglicht wird;
- defensive Schnittstellen, die es dem System und seinen Teilsystemen ermöglichen, verfälschte Eingangswerte und/oder fehlerhafte Interaktionen zu identifizieren;
- On-line Validierung redundanter Eingangssignale, die als Eingangsdaten für die nachfolgende Verarbeitung verwendet werden; und
- genau definierte Verhaltensvorschriften für den Fall einer Ausfallerkennung, die es dem System ermöglichen, sein Potential gegen die Ausbreitung von Ausfällen und/oder entsprechende Auswirkungen zu reduzieren.

DIN V VDE 0801	6.2.2, B .2.2.2	☑	☑	1395
----------------	-----------------	---	---	------

Als mögliche Maßnahmen zur Beherrschung von Fehlern auf rechnerexternen Datenwegen (Informationsaustausch zwischen Rechnern) werden aufgeführt

Anforderung

Stichwort

c) Anforderung an die Auslegung

- Einbit-Hardware-Redundanz (Erweiterung des Busses um ein Bit zur Fehlererkennung)
- Mehrbit-Hardware-Redundanz (Erweiterung des Busses um mehrere Bits zur Fehlererkennung)
- vollständige Hardware Redundanz zur Fehlererkennung, (ambivalente Signale)
- Prüfung über Testmuster
- Test durch Übertragungsprotokolle (Überwachung der Einhaltung der Übermittlungsvorschriften)
- Zeitredundanz (zweimalige serielle Übertragung)
- Informationsredundanz (z. B. Prüfsummen)
- Anwendung des Ruhestromprinzips
- elektrische Leitungen von Informationsleitungen trennen
- bei redundanten Leitungen auf räumliche Trennung achten; Kabelwege dürfen nur Leitungen derselben Redundanzgruppe enthalten
- Erhöhung der Störfestigkeit

Stichwort

d) Anforderung an die Qualitätssicherung

IEC61513

5.3.1.5.6



1089

Um das Potential des CCF komplexer Systeme zu minimieren, muss bei der Auslegung der leittechnischen Architektur eine Analyse eingeschlossen werden, um zu zeigen, dass der Umfang von Rechneranwendungen im Vergleich zu festverdrahteten Systemen und das Mass an Eingriffen des Personals für die Sicherheit akzeptabel sind.



**Anhang III.4 Gewährleistung der Unabhängigkeit der kommunizierenden
Teilsysteme (7 Seiten)**

Anforderungen an Interfaces:

Gewährleistung der Unabhängigkeit der kommunizierenden Teilsysteme

Dokumentenstelle

Kat. A Kat. B

ID

Anforderung

Stichwort

c) Anforderung an die Auslegung

RSK-LL	7.3.5 (2)	☒	☒	461
Die redundanten Stränge der Sicherheitsleittechnik müssen voneinander unabhängig sein, so dass ein anlageninternes versagenauslösendes Ereignis nicht zum Ausfall mehrerer redundanter Stränge des Sicherheitssystems führen kann. Bei Ausfall einzelner Stränge der Sicherheitsleittechnik durch Einwirkungen von außen müssen die übrigen Stränge zur Beherrschung des jeweiligen Störfalls ausreichen.				
RSK-LL	7.2.1 (12)	☒	☐	602
Es ist sicherzustellen, dass eine gleichzeitige Prüfung redundant vorhandener Einrichtungen des Sicherheitssystems verhindert wird. Ein Ausfall darf nur die Funktion eines der zueinander redundanten Stränge des Sicherheitssystems beeinträchtigen.				
KTA 3501	7 (2)	☐	☒	279
Die Zustandsbegrenzungen sind redundant aufzubauen und rückwirkungsfrei gegeneinander und gegen die Betriebssysteme zu entkoppeln.				
KTA 3501	4.6 (3)	☒	☒	174
An Verbindungsstellen zwischen mehreren Redundanzgruppen des Reaktorschutzsystems, wie sie z. B. an Vergleichs-, Wertungs- und Mittelwerteinheiten auftreten, ist die Unabhängigkeit von verschiedenen Redundanzgruppen durch Entkopplung sicherzustellen. Die Entkopplungsglieder müssen die Redundanzgruppen gegeneinander rückwirkungsfrei abgrenzen. (gilt auch für Schutzbegrenzungen)				
KTA 3904	2.2 (4)	☒	☒	425
Redundante Einrichtungen (wie zum Beispiel Anzeigen der Sicherheitsgefahrenmeldeanlage) sind so anzuordnen und aufzubauen, dass trotz eines gerätetechnischen Einzelfehlers, wie Bauelementausfall, eine sicherheitstechnisch ausreichende Anzahl von Einrichtungen betriebsfähig bleibt.				
VDI/VDE 3527	3.4	☒	☐	1195

Stichwort

c) Anforderung an die Auslegung

Bei rechnerbasierten Leittechnik-Systemen bestehen neben Verbindungen über dedizierte Einzelleitungen zumeist auch datentechnische Kommunikations-Verbindungen über Netzwerke oder Punkt-zu-Punkt-Datenverbindungen. Durch die projektierte Realisierung dieser Kommunikationsabläufe und deren Einbindung in die Bearbeitung der leittechnischen Funktionen muss die Unabhängigkeit der Kommunikationsverbindungen von der sicherheitstechnisch wichtigen Bearbeitung der leittechnischen Funktionen weitestgehend sichergestellt werden. Folgende Aspekte sind zu betrachten:

- Die Programmbearbeitung der leittechnischen Funktionen soll möglichst unabhängig von den zu verarbeitenden oder zu übertragenden Daten sein.
- Als fehlerhaft erkannte Signale sind zu kennzeichnen und ihre Ausbreitung ist einzugrenzen. Hierbei ist das Fail-Safe-Verhalten zu beachten.
- Für die übertragenen Daten müssen Datenüberlauf und /oder Messbereichsüberlauf von der Software beherrscht werden, um eine eventuelle Unterbrechung der zyklischen Bearbeitung oder die Beeinträchtigung anderer Leittechnikfunktionen auf diesem Rechner, z. B. durch Zugriff auf falsche Speicherbereiche zu verhindern.
- Die Datenkommunikation muss zeitlich entkoppelt und möglichst ohne eine Synchronisation der kommunizierenden Rechner untereinander realisiert werden, um bei einem Ausfall eines Kommunikationsteilnehmers den Weiterbetrieb der anderen Teilnehmer sicherzustellen.

VDI/VDE 3527 3.4 ☒ ☐ 1194

Die konsequente Realisierung des Defence-in-Depth Prinzips und eines hohen Redundanzgrades bei der Auslegung der Leittechnik führt nicht zwangsläufig zur gewünschten Fehlertoleranz, wenn nicht wirksame Maßnahmen zur Verhinderung einer Fehlerausbreitung vorgesehen werden. Hierbei sind nicht nur Fehlerausbreitungsmechanismen zu betrachten, durch die mehrere, redundante Teilsysteme oder Systeme verschiedener leittechnischer Barrieren gleichzeitig beeinflusst werden können, sondern auch solche Fehlerausbreitungsmechanismen, bei denen - vergleichbar dem Dominoeffekt - erst durch den ersten Fehler selbst die energetischen, datentechnischen oder funktionalen Voraussetzungen für Folgefehler geschaffen werden. Gegen letztgenannte Fehler auszulegen bedarf bei komplexen Systemen umfangreicher Analysen zu Fehlereffekten und Fehlerauswirkungen. Zur Sicherstellung der Unabhängigkeit von leittechnischen Teilsystemen im Sinne dieser Richtlinie sind daher unterschiedliche Arten von Sperren zur Fehlerfortpflanzung zu realisieren, um die verschiedenen Barrieren und Redundanten vor einem common-cause-bedingten Versagen zu bewahren und damit die Einhaltung der übergeordneten Schutzziele zu gewährleisten. Der Sinn von funktionalen Barrieren ist die Verhinderung von Auswirkungen des Versagens einer leittechnischen Funktion auf andere leittechnische Funktionen, die aus der Sicht der Verfahrenstechnik unabhängig von der ausgefallenen Funktion wirken sollen. Bei der Auslegung ist hierbei insbesondere das Vorsehen von unabhängigen Komponenten oder Teilsystemen und die geeignete Verteilung der leittechnischen Funktionen auf diese zu beachten.

VDI/VDE 3527 5.2.3 ☒ ☐ 1207

Keine direkte Kommunikation zwischen Leitsystemen, deren Unabhängigkeit gewährleistet sein soll.

VDI/VDE 3527 5.3.2 ☒ ☐ 1219

Konsequente Entkopplung zwischen den Redundanten, sodass ein Überspannungs-Eintrag aus der Schaltanlage oder der Messperipherie auf eine Redundanz begrenzt bleibt. Ebenso ist die Entkopplung zu redundanz-übergreifenden Einrichtungen wie zur Warte oder zum Prozess-Informationssystem sicherzustellen. Für digitale Systeme erfolgt die Entkopplung vorwiegend über Lichtleiter.

Stichwort

c) Anforderung an die Auslegung

IAEA NS-G-1.1 6.12 - 6.14 ☒ ☒ 1304

Rechnersystementwurf

Redundanz in dem Rechnersystem soll im Allgemeinen vorgesehen werden, um die Zuverlässigkeitsanforderungen und die Anforderungen an die Tests während des Betriebs zu erfüllen. Zur Reduzierung von Möglichkeiten eines vernetzten Ausfalls von redundanten Geräten sollen die redundanten Subsysteme elektrisch und physisch getrennt werden. Da das Voting eine gemeinsame Verwendung aller Subsysteme erfordert, soll eine angemessene und ausreichende Zwischenspeicherung verwendet werden, um sicherzustellen, dass die Trennung der redundanten Subsysteme erhalten bleibt. Redundante Subsysteme sollen auch asynchron laufen.

Die Notwendigkeit für die Überbrückung bei der Inbetriebnahme des integrierten Rechnersystems soll berücksichtigt werden, da es Auswirkungen auf das Hardware-Software-Interface haben kann.

IAEA NS-G-1.3 5.58 ☒ ☒ 778

Wenn die Zuverlässigkeit der Daten und der Datenverbindung von großer Bedeutung ist, soll eine geeignete Kommunikationstechnologie gewählt werden. Eine angemessene Berücksichtigung soll der Verwendung von Redundanz bei der Datenverbindung, dem angemessenen Grad an Vertrauenswürdigkeit der Datenverbindung im Allgemeinen und der Fähigkeit der Sende- und Empfangssysteme, Ausfällen in allen möglichen Betriebsarten zu widerstehen, gewidmet werden. Die Verwendung von Datenkommunikation soll nicht die physische oder funktionale Kanalisierung der Verarbeitung oder der logischen Elemente innerhalb der Systemarchitektur vereiteln.

IAEA NS-G-1.3 4.37 ☒ ☒ 686

Unabhängigkeit soll zur Verhinderung von folgenden Ausbreitungsmöglichkeiten von Ausfällen betrachtet werden:

- zwischen oder innerhalb von Systemkomponenten als Auswirkung von PIEs,
- zwischen oder innerhalb von Systemen der gleichen sicherheitstechnischen Bedeutung und
- von Systemen mit geringerer sicherheitstechnischer Bedeutung zu Systemen mit höherer sicherheitstechnischer Bedeutung.

IAEA NS-G-1.3 4.39 ☒ ☒ 688

Redundante Sicherheitsgruppen innerhalb von sicherheitstechnisch wichtigen Leittechniksystemen sollen voneinander unabhängig sein.

IAEA NS-G-1.3 4.40 ☐ ☒ 689

Es soll Unabhängigkeit zwischen redundanten Teilen von sicherheitsrelevanten Systemen bestehen.

IAEA NS-G-1.3 4.41 ☒ ☒ 690

Stichwort

c) Anforderung an die Auslegung

Eine angemessene Unabhängigkeit soll zwischen diversitären Funktionen bestehen. Die Angemessenheit der bestehenden Unabhängigkeit soll gerechtfertigt werden.

IAEA NS-G-1.3	5.54	☒	☒	774
---------------	------	-------------------------------------	-------------------------------------	-----

Sicherheitstechnisch wichtige Datenverbindungskanäle sollen die Anforderungen an die Unabhängigkeit erfüllen.

IEC 60709	4.7	☒	☒	1378
-----------	-----	-------------------------------------	-------------------------------------	------

Gesichtspunkte der Trennung müssen insbesondere in der Realisierungsstrategie zur Erneuerung der Anlage angesprochen werden. Gesichtspunkte, die berücksichtigt werden müssen, umfassen:

- Trennung in Zwischen-Konfigurationen, wenn neue Leittechnik im Rahmen eines Phasenprogramms installiert wird;
- Festlegung von Teilsystemen, die ohne die Notwendigkeit von Zwischen-Schnittstellen separiert werden können;
- Eignung der bisherigen Trennung für die neue Leittechnik (hauptsächlich Empfindlichkeit der digitalen Leittechnik für elektromagnetische Beeinflussung, besondere Temperaturanforderungen und Empfindlichkeit gegenüber radioaktiver Strahlung);
- Einschränkungen der Kabelführung und Analyse der Bedürfnisse neuer Technologien für spezielle Kabeltrassen (Glasfaserkabel, Busleitungen, Trennungsanforderungen).

IEC 60709	4.4.2	☒	☒	1372
-----------	-------	-------------------------------------	-------------------------------------	------

Leittechnisches Gerät schließt von Natur aus die Erzeugung und die Übertragung elektromagnetischer Signale mit ein. Diese Signale können für versehentliche Veränderung oder Beschädigung durch externe Quellen empfänglich sein. Technologische Fortschritte leittechnischer Systeme, speziell die Reduzierung der Signalspannung, können Systeme noch empfindlicher in Hinsicht auf Fehlfunktionen und Beschädigungen machen.

Deshalb muss elektromagnetische Beeinflussung als CCF-Potential für redundante leittechnische Stränge berücksichtigt werden. Trennung ist eine Maßnahme, um die Unabhängigkeit von leittechnischen Signalen zu bewahren und gegen den potentiellen CCF-Effekt der elektromagnetischen Beeinflussung zu schützen.

Die Normen der Reihe IEC 61000 geben Anleitungen zur Auslegung und Prüfung hinsichtlich elektromagnetischer Beeinflussung.

IEC 60709	6.1	☐	☒	1385
-----------	-----	--------------------------	-------------------------------------	------

Redundante Teile von Kategorie-B-Systemen müssen so ausgelegt und installiert sein, dass keines der in 4.2 (Auslegungsfehler) und 4.3 (versagenauslösende Ereignisse in leittechnischen Systemen) angegebenen Einzelereignisse zum Versagen einer Kategorie-B-Funktion führen kann. Die Behandlung der in 4.4 (versagenauslösende Ereignisse innerhalb der Anlage) und 4.5 (externe versagenauslösende Ereignisse) angegebenen versagenauslösenden Ereignissen in Bezug auf Kategorie-B-Systeme muss, wie in den allgemeinen Prinzipien von Abschnitt 4 beschrieben, von Fall zu Fall erfolgen.

IEC 60709	4.3	☒	☒	1370
-----------	-----	-------------------------------------	-------------------------------------	------

Anforderung

Stichwort

c) Anforderung an die Auslegung

Für jedes sicherheitstechnisch wichtige System müssen dort verursachte versagensauslösende Ereignisse in Betracht gezogen werden. Diese Ereignisse sind üblicherweise durch örtlich beschränkte mechanische und elektrische Auswirkungen charakterisiert, die unterschiedliche funktionale Folgen haben können. Einzelausfälle in zentralen leittechnischen Prozessoreinheiten und an Kommunikationsschnittstellen mit Multiplexern können auch das Potenzial zur Erzeugung von Mehrfachausfällen haben.

Der zufällige Ausfall einer leittechnischen Komponente muss in Betracht gezogen werden, und zwar einschließlich der Energie- oder anderer Hilfsversorgung, die zum Fehlverhalten der Komponente führen kann, einschließlich Kurzschlüssen, Unterbrechung der Kontinuität der Stromkreise, Erdschluss, Spannungs- oder Frequenzänderungen, mechanischem Versagen der Komponenten oder örtlichem Feuer.

Die Folgen der aufgrund eines CCF in zwei oder mehreren Komponenten auftretenden Ausfälle, die sich auf redundante Sicherheitsgruppen auswirken, müssen betrachtet werden. Dabei kann es sich um CCF als Folge von Wartungsfehlern, mechanischer Beschädigung oder elektrischer Interferenz handeln. Umwelteinflüsse, Strahlungsschädigung und andere mögliche gemeinsame physikalische Faktoren müssen berücksichtigt werden.

IEC 60709	4.1	☒	☒	1369
-----------	-----	-------------------------------------	-------------------------------------	------

Wo physikalische Trennung verlangt wird, müssen Vorkehrungen gegen eine Ausfallfortpflanzung in Betracht gezogen werden

- für Ausfälle, die als Folge von anzunehmenden versagensauslösenden Ereignissen (AVE) gleichzeitig Komponenten in Mehrfachsystemen betreffen,
- zwischen Systemen, die Funktionen der gleichen Kategorie ausführen,
- zwischen redundanten Sicherheitsgruppen desselben sicherheitstechnisch wichtigen Systems und
- von Systemen mit Funktionen niedrigerer Kategorie zu Systemen mit Funktionen höherer Kategorie und in einigen speziellen Fällen von Systemen mit Funktionen höherer Kategorie zu Systemen mit Funktionen niedrigerer Kategorie.

Die Arten möglicher versagensauslösender Ereignisse in den folgenden Unterabschnitten müssen in Betracht gezogen werden (z. B. ermittelt, dokumentiert und begründet). Geeignete Vorkehrungen müssen für sicherheitstechnisch wichtige leittechnische Systeme getroffen werden, um mögliche Auswirkungen dieser Ereignisse auf ein annehmbares Maß zu beschränken. Betrachtet werden sollten auch die Auswirkungen der Kombination von Ausfallereignissen.

IEC 60709	4.1	☐	☒	1367
-----------	-----	--------------------------	-------------------------------------	------

Systeme, die Funktionen der Kategorie B ausführen, müssen vor physikalischen Folgewirkungen von Fehlern und üblichen Handlungen geschützt werden, die auftreten innerhalb von

- a) redundanten Teilen jener Systeme und
- b) Systemen einer niedrigeren Kategorie.

Die in Betracht gezogenen Fehler müssen die innerhalb des leittechnischen Systems und seiner Stromversorgung auftretenden Fehler umfassen, die als Ergebnis von Ereignissen außerhalb des leittechnischen Systems auftretenden Fehler dürfen unberücksichtigt bleiben. Wenn Funktionen der Kategorie B als Schutz für bestimmte Störfälle vorgesehen sind, müssen die ausführenden Systeme nach den Prinzipien eines Systems für Kategorie-A-Funktionen ausgelegt sein.

Anforderung

Stichwort

c) Anforderung an die Auslegung

IEC 60709

4.1



1366

Systeme, die Funktionen der Kategorie A ausführen, müssen vor physikalischen Folgewirkungen von Fehlern und üblichen Handlungen geschützt werden, die auftreten innerhalb von

a) redundanten Teilen jener Systeme und

b) Systemen einer niedrigeren Kategorie.

Die in Betracht gezogenen Fehler müssen sowohl die innerhalb des leittechnischen Systems und seiner Stromversorgung als auch die als Ergebnis von Ereignissen außerhalb des leittechnischen Systems auftretenden Fehler umfassen.

In manchen Fällen kann es notwendig sein, eine physikalische Trennung zwischen unterschiedlichen Systemen, die Funktionen der Kategorie A ausführen, vorzusehen, wenn Unabhängigkeit zwischen diesen Funktionen gefordert wird.

IEC 60709

5.1



1379

Redundantes Gerät leittechnischer Systeme muss zuweilen im Einflussbereich von fest installierten Brandschutzsystemen angeordnet werden. In diesen Fällen müssen das leittechnische System und seine Geräte sowie das Brandschutzsystem so ausgelegt sein, dass der Betrieb des Brandschutzsystems die Unabhängigkeit redundanter Sicherheitsgruppen nicht beeinträchtigt.

Die Leistungsfähigkeit redundanter Sicherheitsgruppen darf durch Feuer und Rauch, die außerhalb eines sicherheitstechnisch wichtigen leittechnischen Systems entstehen, nicht negativ beeinflusst werden. Dieses muss durch räumliche Trennung, Barrieren oder eine Kombination von beiden sichergestellt werden, wobei folgende Anforderungen einzuhalten sind:

a) Der Raum zwischen redundanten Systemen oder Kabeln darf keine Strukturen, Geräte oder Materialien enthalten, die eine Ausbreitung des Feuers unterstützen könnten.

b) Wenn zwischen redundanten Systemen oder Kabeln Barrieren angeordnet sind, müssen diese eine Feuerfestigkeit entsprechend den Brandschutzbestimmungen aufweisen.

IEC 60709

6.1



1384

Redundante Teile von Kategorie-A-Systemen müssen so ausgelegt und installiert sein, dass keines der in Abschnitt 4 angegebenen Einzelereignisse zum Versagen einer Kategorie-A-Funktion führen kann.

IEC 61226

7.3.2.2



1041

Eine Funktion in dieser Kategorie muss mit redundanten und getrennten Mitteln ausgeführt werden, anderenfalls muss eine Begründung gegeben werden. Eine solche Begründung kann z. B. auf der Fähigkeit eines Systems beruhen, die geforderte Zuverlässigkeit auch ohne die genannten Mittel zu erreichen, auf der Annehmbarkeit der Folgen des Funktionsausfalls oder auf der Verfügbarkeit von genügend Zeit für alternative Maßnahmen bei Funktionsausfall.

IEC 61226

7.3.2.1



1039

Stichwort

c) Anforderung an die Auslegung

Ein leittechnisches System, das Funktionen der Kategorie A ausführt, muss redundant sein. Angemessene Trennung muss vorgesehen sein, um sicherzustellen, dass irgendein interner Störfall redundante Stränge des Systems nicht unwirksam machen kann. Ein Einzelausfall darf nicht zum Versagen der vorgesehenen Sicherheitsfunktion führen, auch nicht während präventiver Instandhaltung oder wiederkehrender Prüfung, Inspektion oder Reparatur. Die Anwendung des Einzelausfallkriteriums muss in Übereinstimmung mit 5.34 bis 5.39 von IAEA NS-R-1 sein.

IEC61513 6.1.2.2 ☒ ☒ 1128

Die Anordnung der Teilsysteme im System muss den Auslegungs-Randbedingungen nach 6.1.1.2 genügen.

Die Anordnung der Teilsysteme im System muss konsistent mit den Anforderungen an die Zuverlässigkeit der Funktionen mit sicherheitstechnischer Bedeutung sein.

Bei der Festlegung der Einbauorte von Teilsystemen in der Anlage und der Übertragungswege zwischen den Teilsystemen sollten die folgenden Faktoren beachtet werden:

- die Auftrennung redundanter Kanäle von Geräten zur Mehrheitsentscheidung kann notwendig sein, um die Auswirkung lokaler Gefährdungen - wie z.B. Feuer - zu reduzieren und, wenn erforderlich, das Einzelfehlerkriterium zu erfüllen (siehe 6.1.1.2.1);
- die Zentralisierung von Funktionen, die Bedeutung für den Zugriffsschutz haben, kann erforderlich werden, um die Anforderung nach Kontrolle nicht-autorisierten Zugangs zu erfüllen.
- die Zentralisierung komplexer Einrichtungen und Geräte kann den Betrieb, die Wiederholungsprüfungen, Wartung und die Kontrolle von Umgebungsbedingungen erleichtern; und
- der Einsatz von Multiplex-Datentransfer kann die Verkabelungskomplexität vermindern.

Wenn Unabhängigkeit gefordert ist, sollte diese erreicht werden durch:

- elektrische Isolation, die durch Lichtleiter, optische Isolatoren oder Kabelschirme erreicht werden kann;
- physikalische Trennung, die durch geeignete Abstände, Barrieren oder eine Kombination aus beiden erreicht werden kann; und
- für rechnerbasierte Systeme Unabhängigkeit der Kommunikation, die durch die Auswahl geeigneter Kommunikationsarchitekturen und Protokolle erreicht werden kann.

Die Systemarchitektur sollte die Wahrscheinlichkeit und die Konsequenzen der Ausbreitung und Nebenwirkungen von Ausfällen minimieren. Die folgenden Techniken können in Betracht gezogen werden:

- interne Isolation, wodurch Ausfälle sich aufgrund des Fehlens von Ausbreitungspfaden und von gemeinsam genutzten Mitteln nicht ausbreiten können;
- Systemüberwachung mit internen (z.B. Selbstüberwachung) oder externen Einrichtungen (z.B. andere Systeme oder Operateure), wodurch die Früherkennung verfälschter Daten und/oder schadhafter Hilfsmittel ermöglicht wird;
- defensive Schnittstellen, die es dem System und seinen Teilsystemen ermöglichen, verfälschte Eingangswerte und/oder fehlerhafte Interaktionen zu identifizieren;
- On-line Validierung redundanter Eingangssignale, die als Eingangsdaten für die nachfolgende Verarbeitung verwendet werden; und
- genau definierte Verhaltensvorschriften für den Fall einer Ausfallerkennung, die es dem System ermöglichen, sein Potential gegen die Ausbreitung von Ausfällen und/oder entsprechende Auswirkungen zu reduzieren.

IEC61513 6.1.1.2.1c,d) ☒ ☐ 1110

Die Auslegung von Klasse 1-Systemen muss genügend Redundanz vorsehen, um das Einzelfehlerkriterium (single failure criterion) bei Betrieb und Wartung zu erfüllen.

Die Auslegung von Klasse 1-Systemen muss Unabhängigkeit zwischen den verschiedenen Redundanzen vorsehen.



Anhang III.5 Realisierung / Performance (4 Seiten)

Anforderungen an Interfaces: Realisierung / Performance

Dokumentenstelle

Kat. A Kat. B

ID

Anforderung

Stichwort

c) Anforderung an die Auslegung

RSK-LL	7.3.2 (13)	☒	☐	623
--------	------------	-------------------------------------	--------------------------	-----

Die Funktionsfähigkeit der Sicherheitsleittechnik ist unabhängig von Art und Umfang der zeitlichen Änderung ihrer Eingangssignale zu gewährleisten.

KTA 3501	5.6	☒	☐	273
----------	-----	-------------------------------------	--------------------------	-----

Die Zusammenschaltung der Geräte des Reaktorschutzsystems ist so auszuführen, dass ein eindeutiger Funktionsablauf sichergestellt ist. Bauteileigenschaften, wie Eigenzeiten, Toleranzen, Drift- und Störfallverhalten dürfen den zeitlichen Ablauf von Befehlen nicht unzulässig beeinflussen.

KTA 3501	5.5.4 (2)	☒	☐	266
----------	-----------	-------------------------------------	--------------------------	-----

Die Befehlsdauer der Einzelantriebssteuerungen einschließlich der zulässigen Abweichungen ist so zu wählen, dass die Mindestbefehlsdauer der Schaltgeräte eingehalten wird.

VDI/VDE 3527	5.2.3	☒	☐	1209
--------------	-------	-------------------------------------	--------------------------	------

Rückwirkungsfreiheit zwischen der strikt zyklischen Bearbeitung der Anwendersoftware in jedem Prozessor und der davon unabhängigen Kommunikation über die Datenbusse. Nach jedem Zyklus werden die Ergebnis-Telegramme ohne Abfrage des Empfängerstatus gesendet.

VDI/VDE 3527	3.4	☒	☐	1195
--------------	-----	-------------------------------------	--------------------------	------

Bei rechnerbasierten Leittechnik-Systemen bestehen neben Verbindungen über dedizierte Einzelleitungen zumeist auch datentechnische Kommunikations-Verbindungen über Netzwerke oder Punkt-zu-Punkt-Datenverbindungen. Durch die projektierte Realisierung dieser Kommunikationsabläufe und deren Einbindung in die Bearbeitung der leittechnischen Funktionen muss die Unabhängigkeit der Kommunikationsverbindungen von der sicherheitstechnisch wichtigen Bearbeitung der leittechnischen Funktionen weitestgehend sichergestellt werden. Folgende Aspekte sind zu betrachten:

- Die Programmbearbeitung der leittechnischen Funktionen soll möglichst unabhängig von den zu verarbeitenden oder zu übertragenden Daten sein.
- Als fehlerhaft erkannte Signale sind zu kennzeichnen und ihre Ausbreitung ist einzugrenzen. Hierbei ist das Fail-Safe-Verhalten zu beachten.
- Für die übertragenen Daten müssen Datenüberlauf und /oder Messbereichsüberlauf von der Software beherrscht werden, um eine eventuelle Unterbrechung der zyklischen Bearbeitung oder die Beeinträchtigung anderer Leittechnikfunktionen auf diesem Rechner, z. B. durch Zugriff auf falsche Speicherbereiche zu verhindern.

Anforderung

Stichwort

c) Anforderung an die Auslegung

- Die Datenkommunikation muss zeitlich entkoppelt und möglichst ohne eine Synchronisation der kommunizierenden Rechner untereinander realisiert werden, um bei einem Ausfall eines Kommunikationsteilnehmers den Weiterbetrieb der anderen Teilnehmer sicherzustellen.

VDI/VDE 3527 5.2.5 ☒ ☐ 1212

Auslegung der digitalen Sicherheits-Leitsysteme so, dass infolge von Anforderungen keine Änderungen in der Arbeitsweise der Systeme erforderlich werden:

- strikt zyklische Bearbeitung der gesamten Anwendersoftware für jeden Prozessor
- strikt zyklische Versendung aller Telegramme, so dass keine Prozessabhängigkeiten durch variable Prozessor- bzw. Buslast entstehen können
- konsequente Vermeidung von prozessabhängigen Interrupts

IAEA NS-G-1.1 6.12 - 6.14 ☒ ☒ 1304

Rechnersystementwurf

Redundanz in dem Rechnersystem soll im Allgemeinen vorgesehen werden, um die Zuverlässigkeitsanforderungen und die Anforderungen an die Tests während des Betriebs zu erfüllen. Zur Reduzierung von Möglichkeiten eines vernetzten Ausfalls von redundanten Geräten sollen die redundanten Subsysteme elektrisch und physisch getrennt werden. Da das Voting eine gemeinsame Verwendung aller Subsysteme erfordert, soll eine angemessene und ausreichende Zwischenspeicherung verwendet werden, um sicherzustellen, dass die Trennung der redundanten Subsysteme erhalten bleibt. Redundante Subsysteme sollen auch asynchron laufen.

Die Notwendigkeit für die Überbrückung bei der Inbetriebnahme des integrierten Rechnersystems soll berücksichtigt werden, da es Auswirkungen auf das Hardware-Software-Interface haben kann.

IAEA NS-G-1.1 6.23 ☒ ☒ 1310

Rechnersystementwurf

Die Kombination von Hardware und Software und anderer Elemente, die das Rechnersystem bilden, soll die erforderliche Genauigkeit und Antwortzeiten erreichen, um die Leistungsfähigkeitsanforderungen an das Gesamtsystem zu erfüllen. Die Analyse der Genauigkeit und des Timings soll alle möglichen Quellen für Verzögerung oder Signalveränderungen berücksichtigen, die durch alle Elemente in der Kette von den Sensoren für den physikalischen Zustand der Anlage bis zum abschließenden Ansteuerungsmechanismus verursacht werden können. Insbesondere soll berücksichtigt werden, dass die Verwendung einer Rechnersystemhardware oder -software zur Aufbereitung der Anlagensignale sich in der Reduzierung der Antwortzeiten auswirken kann.

IAEA NS-G-1.1 6.24 ☒ ☒ 1311

Rechnersystementwurf

Zur Unterstützung der Identifikation und Analyse des Systemantwortverhaltens sollen deterministische Kommunikationsprotokolle und Zuordnungstechniken für die Rechnerressourcen verwendet werden. Die Analyse soll die Worst-Case-Anforderungen des Systems berücksichtigen.

Dokumentenstelle**Kat. A Kat. B****ID****Anforderung****Stichwort**

c) Anforderung an die Auslegung

IAEA NS-G-1.3

5.57



777

Die Kommunikationstechnologie soll so gewählt und geeignet konfiguriert werden, dass sichergestellt ist, dass die Anforderungen an Antwortzeiten unter allen möglichen Bedingungen hinsichtlich Datenbelastung erfüllt werden.

IEC 60709

4.4.1



1371

Änderungen der Umgebungsbedingungen wie Strahlungs-, Temperatur-, Druck- und Feuchtigkeitfelder während Normalbetrieb und unter Störfallbedingungen müssen berücksichtigt werden. Auf einen Geräteraum oder eine Kabeltrasse einwirkendes Feuer oder Rauch ist eine wichtige Umgebungsbedingung. Auch die ungewollte Betätigung eines Feuerbekämpfungssystems muss in Betracht gezogen werden.

IEC61513

6.1.1.2.2



1111

Die Auslegung des rechnerbasierten Systems sollte deterministisches Verhalten sicherstellen, das mit den Anforderungen an die Leistungsfähigkeit der verwirklichten Funktionen in Einklang steht. a)

Die Kommunikationstechnik muss so gewählt und dimensioniert werden, dass die Anforderungen an die Leistungsfähigkeit bei allen Datenmengen, die bei den angenommenen Anlagentransienten erzeugt werden, erfüllt bleiben (einschließlich Meldeschwall infolge des Gesamtausfalls der Stromversorgung). b)

Stichwort

d) Anforderung an die Qualitätssicherung

IAEA NS-G-1.1

5.32



1295

Rechnersystemanforderungen

Die funktionalen und nichtfunktionalen Spezifikationen für die Systemschnittstellen sollen klar für alle möglichen unterschiedlichen Verhaltensweisen des Systems ausgedrückt werden.

IAEA NS-G-1.1

6.33/34



1317

Rechnersystementwurf

Eine Analyse der internen Schnittstellen soll durchgeführt und dokumentiert werden, die zeigt, dass alle Schnittstelleneigenschaften spezifiziert sind. Dies soll Punkte wie die Definition der zu übertragenden Daten, Betrachtungen der Charakteristiken von synchronen und asynchronen Protokollen und die Wahl der Übertragungsraten umfassen.

Die Sicherheitseigenschaften, die nachgewiesen werden sollen, sollen im Rechnersystementwurf identifiziert und als erfüllt bestätigt werden durch die Analyse der Schnittstelleneigenschaften.

IAEA NS-G-1.3

7.58



873

Anforderung

Stichwort

d) Anforderung an die Qualitätssicherung

Für die Sicherheitssysteme sollen Informationen zu den erlaubten maximal benötigten Zeiten und den erwarteten benötigten Zeiten für die Erreichung der erforderlichen Sicherheitsfunktionen vorhanden sein.

IAEA NS-G-1.3	7.55	☒	☒	870
---------------	------	-------------------------------------	-------------------------------------	-----

Eine Beschreibung des Wertebereichs, der Genauigkeit und der Antwortzeit für das Gesamtsystem und für jeden Kanal soll vorgesehen werden.

IAEA NS-G-1.3	7.43	☒	☒	858
---------------	------	-------------------------------------	-------------------------------------	-----

Jede eine spezielle Bandbreite betreffende Einschränkung (wie erforderliche Abtastraten und Datenübertragungsraten), die Rückwirkungen auf die Entwicklung des Systems hat, soll dokumentiert werden.



Anhang III.6 Fehlererkennung und -beherrschung (3 Seiten)

Anforderungen an Interfaces: Fehlererkennung und -beherrschung

Dokumentenstelle

Kat. A Kat. B

ID

Anforderung

Stichwort

a) Allgemeine/Übergeordnete Anforderung

IAEA NS-R-1

5.40

☒

☒

109

Das Prinzip der Fail-Safe-Auslegung muss berücksichtigt und in die Auslegung der sicherheitstechnisch wichtigen Systeme und Komponenten, wo passend, integriert werden: wenn ein System oder eine Komponente ausfällt, müssen die Anlagensysteme so ausgelegt werden, dass sie in einen sicheren Zustand übergehen, ohne dass irgendeine Aktion eingeleitet werden muss.

Stichwort

c) Anforderung an die Auslegung

VDI/VDE 3527

3.4

☒

☐

1195

Bei rechnerbasierten Leittechnik-Systemen bestehen neben Verbindungen über dedizierte Einzelleitungen zumeist auch datentechnische Kommunikations-Verbindungen über Netzwerke oder Punkt-zu-Punkt-Datenverbindungen. Durch die projektierte Realisierung dieser Kommunikationsabläufe und deren Einbindung in die Bearbeitung der leittechnischen Funktionen muss die Unabhängigkeit der Kommunikationsverbindungen von der sicherheitstechnisch wichtigen Bearbeitung der leittechnischen Funktionen weitestgehend sichergestellt werden. Folgende Aspekte sind zu betrachten:

- Die Programmbearbeitung der leittechnischen Funktionen soll möglichst unabhängig von den zu verarbeitenden oder zu übertragenden Daten sein.
- Als fehlerhaft erkannte Signale sind zu kennzeichnen und ihre Ausbreitung ist einzugrenzen. Hierbei ist das Fail-Safe-Verhalten zu beachten.
- Für die übertragenen Daten müssen Datenüberlauf und /oder Messbereichsüberlauf von der Software beherrscht werden, um eine eventuelle Unterbrechung der zyklischen Bearbeitung oder die Beeinträchtigung anderer Leittechnikfunktionen auf diesem Rechner, z. B. durch Zugriff auf falsche Speicherbereiche zu verhindern.
- Die Datenkommunikation muss zeitlich entkoppelt und möglichst ohne eine Synchronisation der kommunizierenden Rechner untereinander realisiert werden, um bei einem Ausfall eines Kommunikationsteilnehmers den Weiterbetrieb der anderen Teilnehmer sicherzustellen.

IAEA NS-G-1.1

5.13

☒

☒

1283

Die Systemschnittstellen wie auch die Schnittstellen zu einem Anlagennetzwerk sollen so ausgelegt werden, dass sie nicht andere Schutzaktionen, die durch externe Systeme durchgeführt werden, gefährden. Fehlfunktionen und Versagen von externen Systemen oder Hilfssystemen sollen bewirken, dass das System in einen sicheren Zustand gebracht wird.

IAEA NS-G-1.3

5.58

☒

☒

778

Anforderung

Stichwort

c) Anforderung an die Auslegung

Wenn die Zuverlässigkeit der Daten und der Datenverbindung von großer Bedeutung ist, soll eine geeignete Kommunikationstechnologie gewählt werden. Eine angemessene Berücksichtigung soll der Verwendung von Redundanz bei der Datenverbindung, dem angemessenen Grad an Vertrauenswürdigkeit der Datenverbindung im Allgemeinen und der Fähigkeit der Sende- und Empfangssysteme, Ausfällen in allen möglichen Betriebsarten zu widerstehen, gewidmet werden. Die Verwendung von Datenkommunikation soll nicht die physische oder funktionale Kanalisierung der Verarbeitung oder der logischen Elemente innerhalb der Systemarchitektur vereiteln.

IAEA NS-G-1.3	5.56	✓	✓	776
---------------	------	---	---	-----

Die gewählte Häufigkeit der Selbstüberwachung der Datenkommunikation soll der Verwendung der Daten und der Anforderungshäufigkeit der durch das System ausgeführten Sicherheitsfunktionen angemessen sein.

IAEA NS-G-1.3	5.55	✓	✓	775
---------------	------	---	---	-----

Die Auslegung der Datenkommunikationssysteme soll für die Erkennung und, soweit praktisch möglich, für die Behebung von Fehlern und für eine Zustandsanzeige der in der Information übertragenen Daten sorgen.

IAEA NS-G-1.3	4.50	✓	✓	694
---------------	------	---	---	-----

Zu Erleichterung der Gesamtauslegung der Sicherheitssysteme sollen die Geräte so weit wie praktisch möglich ein vorhersagbares und offen gelegtes Ausfallverhalten aufweisen. Die wahrscheinlichsten Ausfallarten in einem sicherheitstechnisch wichtigen System sollen, soweit machbar, das System in einen sicheren Zustand bringen. Es sollen Betrachtungen zur Einbringung von Fail-Safe-Eigenschaften wie Ruhestrom und Watchdog-Timer in die Auslegung durchgeführt werden.

DIN V VDE 0801	6.2.2, B .2.2.2	✓	✓	1395
----------------	-----------------	---	---	------

Als mögliche Maßnahmen zur Beherrschung von Fehlern auf rechnerexternen Datenwegen (Informationsaustausch zwischen Rechnern) werden aufgeführt

- Einbit-Hardware-Redundanz (Erweiterung des Busses um ein Bit zur Fehlererkennung)
- Mehrbit-Hardware-Redundanz (Erweiterung des Busses um mehrere Bits zur Fehlererkennung)
- vollständige Hardware Redundanz zur Fehlererkennung, (ambivalente Signale)
- Prüfung über Testmuster
- Test durch Übertragungsprotokolle (Überwachung der Einhaltung der Übermittlungsvorschriften)
- Zeitredundanz (zweimalige serielle Übertragung)
- Informationsredundanz (z. B. Prüfsummen)
- Anwendung des Ruhestromprinzips
- elektrische Leitungen von Informationsleitungen trennen
- bei redundanten Leitungen auf räumliche Trennung achten; Kabelwege dürfen nur Leitungen derselben Redundanzgruppe enthalten

Stichwort

c) Anforderung an die Auslegung

- Erhöhung der Störfestigkeit



Anhang III.7 Security (1 Seite)

Anforderungen an Interfaces: Security

Dokumentenstelle
Anforderung

Kat. A Kat. B

ID

Stichwort

c) Anforderung an die Auslegung

VDI/VDE 3527	5.5.1	☒	☐	1226
--------------	-------	-------------------------------------	--------------------------	------

Die Sicherung gegen unzulässige Eingriffe kann durch eine Kombination unterschiedlichster Maßnahmen erfolgen wie z. B.

- physischer Zugriffsschutz durch geeignete räumliche Anordnung in verschlossenen Räumen bzw. Schränken
- Sicherung des Zugriffs von Benutzern über hochwertige Authentisierungsverfahren (Kombination von Wissen, Besitz, persönlichen Merkmalen)
- Datentechnische Sicherung der Datenverbindungen, die den physischen Zugriffsschutz durchdringen, z. B. durch Firewall, Application-Gateway, Paketfilter, etc.
- Sicherung von Datenverbindung durch kryptografische Verfahren (Verschlüsselung der Daten)
- Vorsehen von Verriegelungen für Zugriffe über zentrale Geräte zur Prüfung von Freigaben und zur Einschränkung des maximalen gleichzeitigen Zugriffsbereichs (Realisierung z. B. über konventionelle, fest verdrahtete Schaltungen mit Schlüsselschaltern oder über kryptografische Verfahren mittels Chipkarten)

VDI/VDE 3527	3.5	☒	☐	1196
--------------	-----	-------------------------------------	--------------------------	------

Es ist zu verhindern, daß über die vorgesehene Nutzung der Datenverbindungen hinaus Manipulationen möglich sind, die ein Versagen von Sicherheitsfunktionen zur Folge haben können.

Alle für die Security relevanten Maßnahmen sind auf der Basis einer anlagenspezifischen und auf den speziellen Anwendungsfall zugeschnittenen Security-Analyse für die digitale Sicherheits-Leittechnik zu planen.

IAEA NS-G-1.1	3.15	☒	☒	1245
---------------	------	-------------------------------------	-------------------------------------	------

Sicherheitsmanagement von rechnerbasierten Systemen

Es soll nachgewiesen werden, dass Maßnahmen unternommen wurden, um das rechnerbasierte System während seiner gesamten Lebensdauer gegen physische Angriffe, absichtliche oder unbeabsichtigte Zugriffe, Manipulation, Viren und ähnliches zu schützen. Sicherheitssysteme sollen nicht an externe Netzwerke angeschlossen werden, wenn nicht die Begründung gegeben werden kann, dass dies sicher ist.

IAEA NS-G-1.3	4.53	☒	☒	696
---------------	------	-------------------------------------	-------------------------------------	-----

Für die Zugriffskontrolle von rechnerbasierten Systemen sollen Mittel für den beschränkten elektronischen Zugriff auf die Software und auf Daten angewendet werden. Diese Einschränkungen sollen für den Zugriff über Netzwerke und über Wartungsgeräte angewendet werden.



Anhang III.8 Kabel / Kabelverlegung (6 Seiten)

Anforderungen an Interfaces: Kabel / Kabelverlegung

Dokumentenstelle		Kat. A	Kat. B	ID
Anforderung				
Stichwort	c) Anforderung an die Auslegung			
RSK-LL	7.2.1 (10)	☒	☐	600
Leitungen und Kabel sind nach Strängen getrennt und, soweit erforderlich, gegen äußere Einwirkungen geschützt zu verlegen. Leitungen und Kabel zur Signalübertragung und Stromversorgung von redundanten Mess- und Steuereinrichtungen des Sicherheitssystems sollen ohne Einschleifen in Warten oder zentrale Rangierverteiler unmittelbar zu den signalverarbeitenden Baugruppen geführt werden. Sie sind so zu verlegen oder abzuschirmen, dass durch äußere Störquellen, wie z. B. durch Starkstromkabel, eine unzulässige Beeinflussung der Mess- und Steuersignale vermieden wird.				
KTA 3501	5.3.2 (2)	☒	☐	231
Signale zueinander redundanter Einrichtungen dürfen nicht in einem Kabel, einem örtlichen Kabelverteiler und einer Kabeldurchführung geführt werden.				
KTA 3501	5.3.2 (1)	☒	☐	230
Kabel zueinander redundanter Einrichtungen des Reaktorschutzsystems sind nach Abschnitt 5.3.1 (Gesamtsystem) räumlich getrennt oder gegeneinander geschützt zu verlegen.				
VDI/VDE 3527	5.3.2	☒	☐	1219
Konsequente Entkopplung zwischen den Redundanten, sodass ein Überspannungs-Eintrag aus der Schaltanlage oder der Messperipherie auf eine Redundanz begrenzt bleibt. Ebenso ist die Entkopplung zu redundanz-übergreifenden Einrichtungen wie zur Warte oder zum Prozess-Informationssystem sicherzustellen. Für digitale Systeme erfolgt die Entkopplung vorwiegend über Lichtleiter.				
IEC 60709	6.2.5 - .7	☒	☒	1389
Analoge und andere elektrische Signale niedriger Spannung dürfen nicht in denselben Kabelkästen, Umschließungen oder Kanälen verlegt werden wie Energiekabel. Abhängig von der Technologie werden Steuerkabel für Schaltgeräte mit hoher oder niedriger Spannung betrieben; sie müssen daher entsprechend der vorgenannten Anforderung behandelt werden. Glasfaserkabel dürfen zusammen mit Energiekabeln verlegt werden, wenn ihr mechanischer Schutz sichergestellt ist.				
Kabel dürfen nicht in der Nähe von Rohren oder in Kästen, Umschließungen oder Kanälen mit Rohren verlegt werden, die unter Druck und/oder unter höheren Temperaturen stehende				

Stichwort

c) Anforderung an die Auslegung

Medien wie z. B. Öl, Dampf, Wasser, flüssige Metalle befördern oder andere Medien durchleiten, die bei Leckagen oder Rohrbrüchen die Kabel beschädigen können. Ausgenommen davon sind Messfühler- und Stellgliedkabel, bei denen die Nähe zu den Rohrleitungen unvermeidbar ist, um Messfühler oder Stellglieder in den verfahrenstechnischen Prozess einzubinden.

Soweit wie möglich sollten alle Kabel sicherheitstechnisch wichtiger Systeme auf ungefährdeten Trassen in einer Art verlegt werden, die ihre Integrität sicherstellt.

IEC 60709	6.2.1 -6.2.2	✓	✓	1387
-----------	--------------	---	---	------

Trennung von Kabeln ist durch Sicherheitsstrukturen, Barrieren, räumliche Abstände oder durch jede beliebige Kombination dieser Verfahren herzustellen.

Für redundante Kabel in einem sicherheitstechnisch wichtigen leittechnischen System gilt:

- für jede redundante Gruppe müssen physikalisch getrennte Kabelführungen, Kästen, Kanäle, Röhren und Durchführungen vorgesehen sein;
- auf jeder gegebenen Kabeltrasse, jedem Kabelkasten oder Kanal, jeder horizontalen oder vertikalen Kabelröhre oder in jeder Durchführung dürfen nur Kabel derselben redundanten Gruppe verlegt sein;
- bei versagenauslösenden Ereignissen in leittechnischen Systemen, deren Ursache im Kabelsystem liegt, wie Lichtbogen oder Überhitzung durch Kurzschlüsse, Überlastung, Spannungstransienten usw. (siehe 4.3), kann ein geringeres Ausmaß physikalischer Trennung ausreichend sein. Ein horizontaler Abstand von mindestens 30 cm und ein vertikaler Abstand von mindestens 80 cm müssen eingehalten werden. Wo dies nicht der Fall ist, müssen die redundanten Kabel in geschlossenen Trassen, die als Barrieren qualifiziert sind, verlegt werden, oder es muss eine Begründung für die geringeren Abstände gegeben werden;
- für anlageninterne und externe versagenauslösende Ereignisse wie Feuer oder schwere Bauschäden (siehe 4.4 und 4.5) muss eine aufwendigere physikalische Trennung einschließlich Barrieren und/oder Sicherheitseinbauten vorgesehen werden.

Kleinere Abstände als in 6.2.1 angegeben dürfen nach der Analyse der vorgeschlagenen Kabelinstallation zugelassen werden. Die Analyse sollte auf der Grundlage von Tests zur Ermittlung der flammhemmenden Charakteristiken der vorgeschlagenen Kabelinstallation durchgeführt werden, wobei Merkmale wie Isolier- und Mantelmaterialien der Kabel, Füllmaterial für Kabeltrassen, Trassentypen und Anordnungen zu berücksichtigen sind. Für kleinere Abstände in gefährlichen Bereichen sollten das Gefahrenausmaß (wie Größe eines Feuers oder eines Leitungsbruchs) und abschwächende Maßnahmen (wie Sprinkler) in Betracht gezogen werden.

IEC 60709	5.3	✓	✓	1381
-----------	-----	---	---	------

Wenn Signale von Geräten eines Kategorie-A-Systems(N1) zu Systemen mit niedrigerer Kategorie übertragen werden, muss dies über Isolationseinrichtungen geschehen, die dem Kategorie-A-System angehören. Die Isolationseinrichtung muss so ausgelegt sein, dass Ausfälle oder Bedingungen an ihren Ausgängen (die mit den Systemen niedrigerer Kategorie verbunden sind) eine Sicherheitsaktion des Kategorie-A-Systems oder -Teilsystems, mit der die Isolationseinrichtung verbunden ist, nicht verhindern können. Die vorgesehene elektrische Isolationseinrichtung muss die Anforderungen in 5.3.2 erfüllen.

Für Wartungszwecke müssen zeitweise Verbindungen ohne Isolationseinrichtung mit Kategorie-A-Systemen gestattet werden, vorausgesetzt, die Verbindung besteht zu jedem Zeitpunkt

Anforderung**Stichwort**

c) Anforderung an die Auslegung

nur mit einem einzigen Strang eines redundanten Systems, die Verbindung wird nach Gebrauch aufgehoben, und das System ist in der Lage, einen durch Ausfall oder Verwendung der Verbindung eingeschleiften Fehler zu beherrschen.

Es muss ein Schutz gegen folgende Ausfälle und Bedingungen sichergestellt sein:

- a) Kurz- und Erdschlüsse;
- b) Unterbrechungen;
- c) Aufschaltung der maximalen Wechsel- oder Gleichspannung, die vernünftigerweise auftreten kann, wobei die verfügbaren Spannungsquellen und Potentiale in den Kategorie-A-Systemen und sonstigen Systemen in Betracht zu ziehen sind;
- d) elektromagnetische und elektrostatische Beeinflussung.

Hinsichtlich der Eigenschaften einer Isolationseinrichtung sind zu berücksichtigen:

- Toleranz und Isolierung gegenüber elektrischen Schwingungen und Spitzen nach IEC 61000-6-5;
- Toleranz und Isolierung gegenüber elektromagnetischer Beeinflussung nach IEC 61000-6-5;
- einfache Barrieren zur elektrischen Isolierung zwischen nahen oder benachbarten Endverbindungen oder Kontaktgruppen an Relais;
- Vorsorge gegen Übertragung außerordentlich hoher oder zerstörender Spannungen.

In diesem Zusammenhang sollte eine Untersuchung über die maximale Spannung, die unter normalen und fehlerhaften Bedingungen zu erwarten ist, durchgeführt werden, und die möglichen Auswirkungen auf das sicherheitstechnisch wichtige Gerät sollten untersucht werden, wenn diese Spannung auf die Endverbindungen der Isolationseinrichtung auf der Seite der sicherheitstechnisch weniger wichtigen Einrichtungen aufgeschaltet wird.

Weiter sollten Vorkehrungen getroffen werden, um die Möglichkeit zu minimieren, dass Ausfälle in nicht sicherheitsrelevanten Systemen spontane ungewollte Aktionen von Funktionen der Kategorie A auslösen.

Werden Anlagengeräte, die von einem Kategorie-A-System angesteuert werden, auch von Signalen eines Systems niedrigerer Kategorie angesteuert, müssen Isolationseinrichtungen vorgesehen sein, die einen Vorrang der vom Kategorie-A-System ausgehenden Steuersignale sicherstellen. Ausfälle im oder normale Aktionen des Systems niedrigerer Kategorie dürfen die Funktionen des Kategorie-A-Systems unter Anlagenbedingungen, die einen Erfolg dieser Funktionen erfordern, nicht überlagern. Die Isolationseinrichtungen zur Sicherstellung des Vorrangs müssen als Teil des Kategorie-A-Systems eingeordnet sein.

Ausfälle und Fehlbetätigungen in Systemen, die nicht entsprechend Kategorie A eingeordnet sind, dürfen keinerlei Rückwirkungen auf das Ansprechverhalten, die Drift, Genauigkeit, Rauschempfindlichkeit oder andere Eigenschaften des Kategorie-A-Systems haben, die seine Fähigkeit beeinträchtigen könnten, die geforderten Sicherheitsfunktionen auszuführen.

Wenn Signale von Kategorie-B-Systemen oder Kategorie-C-Systemen zur Verwendung in Systemen niedrigerer Kategorie ausgekoppelt werden, mögen Isolationseinrichtungen nicht gefordert sein; guter Ingenieurpraxis folgend sollte jedoch die Ausfallfortpflanzung verhindert werden. In Fällen, in denen Kategorie-B-Funktionen ausführende Systeme infolge der

Stichwort

c) Anforderung an die Auslegung

ausgeführten Funktionen Aspekte von Kategorie-A-Systemen zu berücksichtigen haben, muss eine Isolation vorgesehen werden.

Glasfaserkabel stellen ein sehr wirksames Mittel zur Erzielung elektrischer Isolation dar und sollten, wenn immer möglich, verwendet werden.

IEC 60709	5.1		☑	☑	1379
-----------	-----	--	---	---	------

Redundantes Gerät leittechnischer Systeme muss zuweilen im Einflussbereich von fest installierten Brandschutzsystemen angeordnet werden. In diesen Fällen müssen das leittechnische System und seine Geräte sowie das Brandschutzsystem so ausgelegt sein, dass der Betrieb des Brandschutzsystems die Unabhängigkeit redundanter Sicherheitsgruppen nicht beeinträchtigt.

Die Leistungsfähigkeit redundanter Sicherheitsgruppen darf durch Feuer und Rauch, die außerhalb eines sicherheitstechnisch wichtigen leittechnischen Systems entstehen, nicht negativ beeinflusst werden. Dieses muss durch räumliche Trennung, Barrieren oder eine Kombination von beiden sichergestellt werden, wobei folgende Anforderungen einzuhalten sind:

- a) Der Raum zwischen redundanten Systemen oder Kabeln darf keine Strukturen, Geräte oder Materialien enthalten, die eine Ausbreitung des Feuers unterstützen könnten.
- b) Wenn zwischen redundanten Systemen oder Kabeln Barrieren angeordnet sind, müssen diese eine Feuerfestigkeit entsprechend den Brandschutzbestimmungen aufweisen.

IEC 60709	4.7		☑	☑	1378
-----------	-----	--	---	---	------

Gesichtspunkte der Trennung müssen insbesondere in der Realisierungsstrategie zur Erneuerung der Anlage angesprochen werden. Gesichtspunkte, die berücksichtigt werden müssen, umfassen:

- Trennung in Zwischen-Konfigurationen, wenn neue Leittechnik im Rahmen eines Phasenprogramms installiert wird;
- Festlegung von Teilsystemen, die ohne die Notwendigkeit von Zwischen-Schnittstellen separiert werden können;
- Eignung der bisherigen Trennung für die neue Leittechnik (hauptsächlich Empfindlichkeit der digitalen Leittechnik für elektromagnetische Beeinflussung, besondere Temperaturanforderungen und Empfindlichkeit gegenüber radioaktiver Strahlung);
- Einschränkungen der Kabelführung und Analyse der Bedürfnisse neuer Technologien für spezielle Kabeltrassen (Glasfaserkabel, Busleitungen, Trennungsanforderungen).

IEC 60709	4.4.1		☑	☑	1371
-----------	-------	--	---	---	------

Änderungen der Umgebungsbedingungen wie Strahlungs-, Temperatur-, Druck- und Feuchtigkeitfelder während Normalbetrieb und unter Störfallbedingungen müssen berücksichtigt werden. Auf einen Geräteraum oder eine Kabeltrasse einwirkendes Feuer oder Rauch ist eine wichtige Umgebungsbedingung. Auch die ungewollte Betätigung eines Feuerbekämpfungssystems muss in Betracht gezogen werden.

IEC61513	6.1.2.2		☑	☑	1128
----------	---------	--	---	---	------

Die Anordnung der Teilsysteme im System muss den Auslegungs-Randbedingungen nach 6.1.1.2 genügen.

Anforderung

Stichwort

c) Anforderung an die Auslegung

Die Anordnung der Teilsysteme im System muss konsistent mit den Anforderungen an die Zuverlässigkeit der Funktionen mit sicherheitstechnischer Bedeutung sein.

Bei der Festlegung der Einbauorte von Teilsystemen in der Anlage und der Übertragungswege zwischen den Teilsystemen sollten die folgenden Faktoren beachtet werden:

- die Auftrennung redundanter Kanäle von Geräten zur Mehrheitsentscheidung kann notwendig sein, um die Auswirkung lokaler Gefährdungen - wie z.B. Feuer - zu reduzieren und, wenn erforderlich, das Einzelfehlerkriterium zu erfüllen (siehe 6.1.1.2.1);
- die Zentralisierung von Funktionen, die Bedeutung für den Zugriffsschutz haben, kann erforderlich werden, um die Anforderung nach Kontrolle nicht-autorisierten Zugangs zu erfüllen.
- die Zentralisierung komplexer Einrichtungen und Geräte kann den Betrieb, die Wiederholungsprüfungen, Wartung und die Kontrolle von Umgebungsbedingungen erleichtern; und
- der Einsatz von Multiplex-Datentransfer kann die Verkabelungskomplexität vermindern.

Wenn Unabhängigkeit gefordert ist, sollte diese erreicht werden durch:

- elektrische Isolation, die durch Lichtleiter, optische Isolatoren oder Kabelschirme erreicht werden kann;
- physikalische Trennung, die durch geeignete Abstände, Barrieren oder eine Kombination aus beiden erreicht werden kann; und
- für rechnerbasierte Systeme Unabhängigkeit der Kommunikation, die durch die Auswahl geeigneter Kommunikationsarchitekturen und Protokolle erreicht werden kann.

Die Systemarchitektur sollte die Wahrscheinlichkeit und die Konsequenzen der Ausbreitung und Nebenwirkungen von Ausfällen minimieren. Die folgenden Techniken können in Betracht gezogen werden:

- interne Isolation, wodurch Ausfälle sich aufgrund des Fehlens von Ausbreitungspfaden und von gemeinsam genutzten Mitteln nicht ausbreiten können;
- Systemüberwachung mit internen (z.B. Selbstüberwachung) oder externen Einrichtungen (z.B. andere Systeme oder Operateure), wodurch die Früherkennung verfälschter Daten und/oder schadhafter Hilfsmittel ermöglicht wird;
- defensive Schnittstellen, die es dem System und seinen Teilsystemen ermöglichen, verfälschte Eingangswerte und/oder fehlerhafte Interaktionen zu identifizieren;
- On-line Validierung redundanter Eingangssignale, die als Eingangsdaten für die nachfolgende Verarbeitung verwendet werden; und
- genau definierte Verhaltensvorschriften für den Fall einer Ausfallerkennung, die es dem System ermöglichen, sein Potential gegen die Ausbreitung von Ausfällen und/oder entsprechende Auswirkungen zu reduzieren.

DIN V VDE 0801 6.2.2, B .2.2.2



1395

Als mögliche Maßnahmen zur Beherrschung von Fehlern auf rechnerexternen Datenwegen (Informationsaustausch zwischen Rechnern) werden aufgeführt

- Einbit-Hardware-Redundanz (Erweiterung des Busses um ein Bit zur Fehlererkennung)
- Mehrbit-Hardware-Redundanz (Erweiterung des Busses um mehrere Bits zur Fehlererkennung)
- vollständige Hardware Redundanz zur Fehlererkennung, (ambivalente Signale)
- Prüfung über Testmuster
- Test durch Übertragungsprotokolle (Überwachung der Einhaltung der Übermittlungsvorschriften)
- Zeitredundanz (zweimalige serielle Übertragung)
- Informationsredundanz (z. B. Prüfsummen)
- Anwendung des Ruhestromprinzips
- elektrische Leitungen von Informationsleitungen trennen
- bei redundanten Leitungen auf räumliche Trennung achten; Kabelwege dürfen nur Leitungen derselben Redundanzgruppe enthalten

Stichwort

c) Anforderung an die Auslegung

- Erhöhung der Störfestigkeit